WatchGuard® Firebox® X Edge e-Series User Guide

Firebox X Edge e-Series - Firmware Version 8.0
All Firebox X Edge e-Series Standard and Wireless Models

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2006 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in an appendix at the end of this book. You can also find it online at:
http://www.watchguard.com/help/documentation/

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This product is for indoor use only.

WatchGuard Firebox Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this

AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR

OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AD// (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 040226

Firmware Version: 8.0
Part Number: 1776-0000
Guide Version: 8.0

Abbreviations Used in this Guide

3DES	Triple Data Encryption Standard
BOVPN	Branch Office Virtual Private Network
DES	Data Encryption Standard
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
MAC	Media Access Control
MUVPN	Mobile User Virtual Private Network
NAT	Network Address Translation
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WSEP	WatchGuard Security Event Processor

Contents

CHAPTER 1 Introduction to Network Security 1
Network Security 1
About Networks 1
Clients and servers 1
Connecting to the Internet 2
Protocols 2
How Information Travels on the Internet 3
IP Addresses 3
Network addressing 4
About DHCP 4
About PPPoE 4
Default gateway 4
Domain Name Service (DNS) 4
Services 4
Ports 5
Firewalls 6
The Firebox® X Edge and Your Network 7
CHAPTER 2 Installing the Firebox X Edge e-Series 9
Installation Requirements 9
Package Contents 9
Identifying Your Network Settings 10
About network addressing 10
Static addresses, DHCP, and PPPoE 10

TCP/IP properties 11
PPPoE settings 12
Web Browser HTTP Proxy Settings 13
Web Browser Pop-up Blocking Settings 14
Connecting the Firebox X Edge 15
Connecting the Edge to more than four devices 15
About session licenses 16
Setting Your Computer to Connect to the Edge 17
If your computer gets its address from DHCP 17
If your computer has a static IP address 18
Using the Quick Setup Wizard 18
Registering and Activating LiveSecurity Service 20

CHAPTER 3 Navigating the Firebox X Edge e-Series Configuration Pages 21
Navigating the Configuration Pages 22
Using the navigation bar 23
Configuration Overview 24
System Status page 24
Network page 25
Firebox Users page 26
Administration page 26
Firewall page 27
Logging page 28
WebBlocker page 29
VPN page 29
Wizards page 30

CHAPTER 4 Configuration and Management Basics 33
Factory Default Settings 33
Restoring the Firebox to the factory default settings 34
Restarting the Firebox 34
Local restart 35
Remote reboot 35
Setting the System Time 35
Selecting HTTP or HTTPS for Management 37
Changing the HTTP Server Port 37
Setting up WatchGuard System Manager Access 38
Rename the Firebox X Edge e-Series 38
Enable remote management with WSM v8.3.1 or higher 38
Enable remote management with WFS v7.3 or earlier 40

Updating the Firebox X Edge Software 41
Method 1: Installing software automatically 41
Method 2: Installing software manually 42
Activating Upgrade Options 42
Upgrade options 43
Enabling the Model Upgrade Option 44
Viewing the Configuration File 44
CHAPTER 5 Changing Your Network Settings 45
Using the Network Setup Wizard 45
Configuring the External Network 46
If your ISP uses DHCP 46
If your ISP uses static IP addresses 47
If your ISP uses PPPoE 48
Configuring the Trusted Network 50
Changing the IP address of the trusted network 50
Using DHCP on the trusted network 51
Setting trusted network DHCP address reservations 51
Configuring the trusted network for DHCP relay 52
Using static IP addresses for trusted computers 53
Adding computers to the trusted network 53
Configuring the Optional Network 53
Enabling the optional network 54
Changing the IP address of the optional network 54
Using DHCP on the optional network 55
Setting optional network DHCP address reservations 56
Configuring the optional network for DHCP relay 56
Using static IP addresses for optional computers 57
Adding computers to the optional network 57
Making Static Routes 57
Registering with the Dynamic DNS Service 58
Enabling the WAN Failover Option 60
Using the WAN Failover Setup Wizard 61
Using the Network page 61
If you are using a broadband connection for failover 61
Configuring BIDS 63
CHAPTER 6 Firebox X Edge e-Series Wireless Setup 65
Connecting to the Firebox X Edge e-Series Wireless 65
Using the Wireless Network Wizard 66
Configuring Basic Wireless Settings 67

Selecting the wireless network assignment 67
Setting the SSID 68
Setting the operating region and channel 68
Controlling SSID broadcasts 68
Logging authentication events 68
Setting the wireless mode 69
Setting the fragmentation threshold 69
Configuring Wireless Security Settings 69
Setting the wireless authentication method 70
Configuring encryption 70
Configuring wireless clients to use MUVPN 71
Restricting Wireless Access by MAC Address 71
Configuring Wireless Guest Services 72
Enabling guest services 73
Setting password protection 73
Setting network access rules for guests 73
Connecting to the Edge as a wireless guest 74
Configuring the Wireless Card on Your Computer 74
CHAPTER 7 Configuring Firewall Settings 77
About This Chapter 77
About Services 77
Incoming and outgoing traffic 78
Traffic through VPN tunnels 78
Configuring Incoming Services 78
Configuring common services for incoming traffic 79
About custom services for incoming traffic 80
Adding a custom service using the wizard 80
Adding a custom incoming service manually 80
Filter incoming traffic for a custom service 82
Filter outgoing traffic for a custom service 82
Configuring Outgoing Services 83
Configuring common services for outgoing traffic 84
About custom services for outgoing traffic 84
Adding a custom service using the wizard 85
Adding a custom outgoing service manually 85
Filter traffic for an outgoing service 86
Services for the Optional Network 86
Controlling traffic from the trusted to optional network 87
Disabling traffic filters between trusted and optional networks 88

Blocking External Sites 89
Configuring Firewall Options 89
Responding to ping requests 90
Denying FTP access to the Firebox X Edge 90
Logging all allowed outgoing traffic 90
Logging denied broadcast traffic 91
Log denied spoofed traffic 91
Changing the MAC address of the external interface 91

CHAPTER 8 Managing Network Traffic 93
About Network Traffic 93
Causes for slow network traffic 93
Traffic Categories 94
Interactive traffic 94
High priority 94
Medium priority 94
Low priority 94
Configuring Traffic Control 94
Enable traffic control 95
Add a traffic control filter 96
Edit a traffic control filter 97
Change the priority of a traffic control filter 97
Remove a traffic control filter 97
Working with Firewall NAT 97
NAT types 97
NAT behavior 98
Secondary IP addresses 98
Enable 1-to-1 NAT 99
Add a 1-to-1 NAT entry 99
Add or Edit a Custom Service for 1-to-1 NAT 100
Remove a 1-to-1 NAT entry 101

CHAPTER 9 Configuring Logging and System Time 103
Viewing Log Messages 103
Log to a WatchGuard Log Server 104
Logging to a Syslog Host 105

CHAPTER 10 Managing Users and Groups 107
Seeing Current Sessions and Users 107
Firebox Users Settings 107
Active Sessions 108
Stopping a session 108

Local User Accounts 109
About User Licenses 110
About User Authentication 110
Setting authentication options for all users 110
Configuring MUVPN client settings 112
Authenticating to the Edge 112
Using Local Firebox Authentication 113
Creating a read-only administrative account 114
Setting a WebBlocker profile for a user 114
Enabling MUVPN for a user 115
The Administrator account 115
Changing a user account name or password 115
Using LDAP/Active Directory Authentication 116
Configuring the LDAP/Active Directory authentication service 116
Using the LDAP authentication test feature 118
Configuring groups for LDAP authentication 118
Adding a group 118
Setting a WebBlocker profile for a user 119
LDAP Authentication and MUVPN 120
Allowing Internal Hosts to Bypass User Authentication 120

CHAPTER 11 Configuring WebBlocker 121
How WebBlocker Works 121
Configuring Global WebBlocker Settings 121
Creating WebBlocker Profiles 123
WebBlocker Categories 124
Allowing Certain Sites to Bypass WebBlocker 132
Blocking Additional Web Sites 132
Bypassing WebBlocker 133

CHAPTER 12 Configuring Virtual Private Networks 135
About This Chapter 135
What You Need to Create a VPN 135
Managed VPN 136
Manual VPN: Setting Up Manual VPN Tunnels 137
What you need for Manual VPN 137
Phase 1 settings 139
Phase 2 settings 141
VPN Keep Alive 142
Viewing VPN Statistics 143

Frequently Asked Questions 143
CHAPTER 13 Configuring the MUVPN Client 145
About This Chapter 145
Enabling MUVPN for Firebox X Edge e-Series Users 146
Configuring MUVPN client settings 146
Enabling MUVPN access for a Firebox user account 147
Configuring the Edge for MUVPN clients using a Pocket PC ...148
Distributing the Software and the .wgx File 148
Preparing Remote Computers for MUVPN 149
WINS and DNS servers 149
Windows NT setup 150
Windows 2000 setup 151
Windows XP setup 152
Installing and Configuring the MUVPN Client 154
Installing the MUVPN client 154
Uninstalling the MUVPN client 155
Connecting and Disconnecting the MUVPN Client 156
Connecting the MUVPN client 156
The MUVPN client icon 156
Allowing the MUVPN client through a personal firewall 157
Disconnecting the MUVPN client 157
Monitoring the MUVPN Client Connection 158
Using Log Viewer 158
Using Connection Monitor 158
The ZoneAlarm Personal Firewall 159
Allowing traffic through ZoneAlarm 159
Shutting down ZoneAlarm 160
Uninstalling ZoneAlarm 160
Using MUVPN on a Firebox X Edge e-Series Wireless Network .161
Tips for Configuring the Pocket PC 162
Troubleshooting Tips 163
APPENDIX A Firebox X Edge e-Series Hardware.....165
Package Contents 165
Specifications 166
Hardware Description 167
Front panel 167
Rear view 168
Side panels 168

AC Power Adapter 169
About the Firebox X Edge e-Series Wireless. 169
Antenna directional gain 170
Signal attenuation 170
Channel data rate 170
APPENDIX B Legal Notifications 171
Copyright, Trademark, and Patent Information 171
General Information 171
OpenSSL 171
OpenLDAP 173
Lua 173
NCFTP 174
DHCP 175
bzip2 176
libexpat 176
lsof 177
libarchive 177
zlib 177
sasl 178
pppd 178
OpenNTPD 183
JFFS2, ProCPS, iputils 184
PCRE 189
Traceroute 190
Redboot 190
Certifications and Notices 196
WEEE Statement: 196
RoHS Statement: 196
FCC Certification 196
FCC Part 68 Statement (DSL Version) 197
CE Notice 198
Industry Canada 198
CANADA RSS-210 198
France 198
Class A Korean Notice 199
VCCI Notice Class A ITE 199
Taiwanese Class A Notice 199
Taiwanese Wireless Notice 199
Declaration of Conformity 200
Limited Hardware Warranty 200

CHAPTER 1 Introduction to Network Security

Thank you for your purchase of the WatchGuard® Firebox® X Edge e-Series. This security device helps protect your computer network from threat and attack.

This chapter gives you basic information about networks and network security. This information can help you when you configure the Firebox X Edge. If you are experienced with computer networks, we recommend that you go to the subsequent chapter.

Network Security

While the Internet gives you access to a large quantity of information and business opportunity, it also opens your network to attackers. A good network security policy helps you find and prevent attacks to your computer or network.

Many people think that their computer holds no important information. They do not think that their computer is a target for a hacker. This is not correct. A hacker can use your computer as a platform to attack other computers or networks or use your account information to send e-mail spam or attacks. Your account information is also vulnerable and valuable to hackers.

About Networks

A *network* is a group of computers and other devices that are connected to each other. It can be two computers that you connect with a serial cable, or many computers around the world connected through the Internet. Computers on the same network can do work together and share data.

A LAN *(Local Area Network)* is a connected group of computers that use the same method of communication to share data.

A WAN *(Wide Area Network)* is a connected group of computers that can be far apart in different locations.

Clients and servers

Clients and servers are components of a network. A *server* is a computer that makes its resources available to the network. Some of these resources are documents, printers, and programs. A *client* is a computer that uses the resources made available by the server.

Connecting to the Internet

ISPs (Internet service providers) are companies that give access to the Internet through network connections. *Bandwidth* is the rate at which a network connection can send data: for example, 3 megabits per second (Mbps).

A high-speed Internet connection, such as a cable modem or a DSL (Digital Subscriber Line), is known as a *broadband* connection. Broadband connections are much faster than dial-up connections: the bandwidth of a dial-up connection is less than .1 Mbps, while a cable modem can be 5 Mbps or more.

Typical speeds for cable modems are usually lower than the maximum speeds, because each person in a neighborhood is a member of a LAN. Each computer in that LAN uses some of the bandwidth. Because of this "shared-medium" system, cable modem connections can become slow when more users are on the network.

DSL connections supply constant bandwidth, but they are usually slower than cable modem connections. Also, the bandwidth is only constant between your home or office and the DSL central office. The DSL central office cannot supply a constant connection to a Web site or network.

Protocols

A *protocol* is a group of rules that allow computers to connect across a network. Protocols are the "grammar" that computers use to speak to each other.

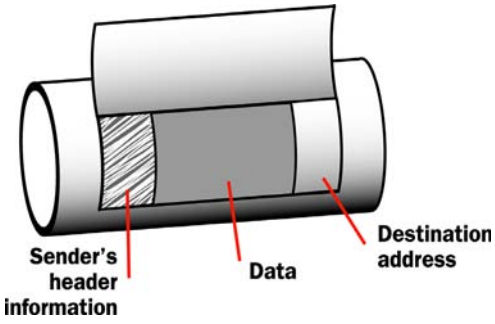
The standard protocol when you connect to the Internet is the IP (Internet Protocol). This protocol is the usual language of computers on the Internet.

A protocol also tells how data is sent through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

TCP/IP is the basic protocol used by computers that connect to the Internet. You must know some settings of TCP/IP when you set up your Firebox® X Edge. For more information on TCP/IP, see "Finding your TCP/IP properties" on page 15.

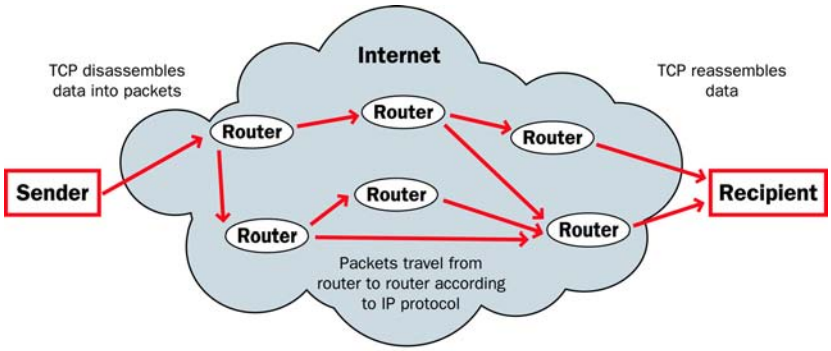
How Information Travels on the Internet

The data that you send through the Internet is cut into units, or packets. Each packet includes the Internet address of the destination. The packets that make up a connection can use different routes through the Internet. When they all get to their destination, they are assembled back into a file. To make sure that the packets get to the destination, address information is added to the packets.



Data packet

The TCP and IP protocols are used to send and receive these packets. TCP disassembles the data and assembles it again. IP adds information to the packets, such as the sender, the recipient, and any special instructions.



Packets traveling on the Internet

IP Addresses

To send mail to a person, you must first know their physical address. For a computer to send data to a different computer, it must first know the address of that computer. A computer address is known as an *IP address*. Only one device can use an IP address at a time.

An IP address is a group of four numbers divided by decimal points. Some examples of IP addresses are:

- 192.168.0.11
- 10.1.20.18
- 208.15.15.15

Network addressing

ISPs (Internet service providers) assign an IP address to each device on their network. The IP address can be static or dynamic. Each ISP has a small number of IP addresses.

Static IP addresses are permanently assigned to a device. These addresses do not change automatically, and are frequently used for servers.

Dynamic IP addresses change with time. If a dynamic address is not in use, it can be automatically assigned to a different device.

Your ISP can tell you how their system assigns IP addresses.

About DHCP

Many ISPs assign dynamic IP addresses through DHCP (Dynamic Host Configuration Protocol). When a computer connects to the network, a DHCP server at the ISP assigns that computer an IP address. It is not necessary to assign IP addresses manually when you use DHCP.

About PPPoE

Some ISPs assign their IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE expands a standard dial-up connection to add some of the features of Ethernet and PPP. This system allows the ISP to use the billing, authentication, and security systems of their dial-up infrastructure with DSL modem and cable modem products.

Default gateway

A default gateway is a node on a computer network that serves as an access point to another network. Usually, the default gateway is the IP address of the router that is between your network and the Internet. After you install the Firebox X Edge on your network, the Edge acts as the default gateway for all computers connected to its trusted or optional interfaces.

Domain Name Service (DNS)

If you do not know the address of a person, you can frequently find it in the telephone directory. On the Internet, the equivalent to a telephone directory is the DNS (Domain Name Service). Each Web site has a domain name (such as "mysite.com") that is equal to an IP address. When you type a domain name to show a Web site, your computer gets the IP address from a DNS server.

A URL (Uniform Resource Locator) includes a domain name and a protocol. An example of a URL is:

http://www.watchguard.com/

In summary, the DNS is the system that translates Internet domain names into IP addresses. A DNS server is a server that performs this translation.

Services

A *service* opens access from your network to a computer that is external to your network. You use services to send e-mail or move files from one computer to a different computer through the network. These services use protocols. Frequently used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- E-mail uses Simple Mail Transfer Protocol (SMTP)
- File transfer uses File Transfer Protocol (FTP)
- Changing a domain name to an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or SSH (Secure Shell)

Some services are necessary, but each service you add to your security policy can also add a security risk. To send and receive data, you must "open a door" in your computer, which puts your network at risk. Attackers can use open access of a service to try to get into a network. We recommend that you only add services that are necessary for your business.

Ports

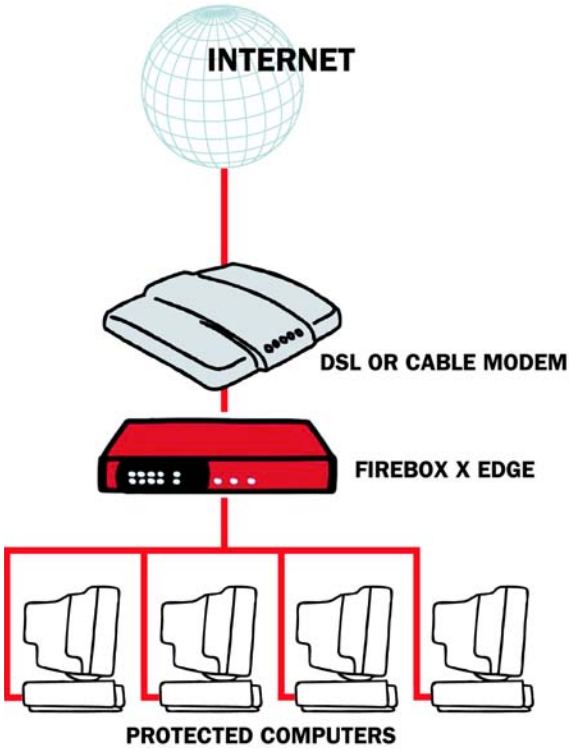
Usually, a port is a connection point where you use a socket and a plug to connect two devices. Computers also have ports that are not physical locations. These ports are where programs transmit data.

Some protocols, such as HTTP, have ports with assigned numbers. For example, most computers transmit e-mail on port 25 because the SMTP protocol is assigned to port 25. Other programs are assigned port numbers dynamically for each connection. The IANA (Internet Assigned Numbers Authority) keeps a list of well known ports. You can see this list at www.iana.org/assignments/port-numbers.

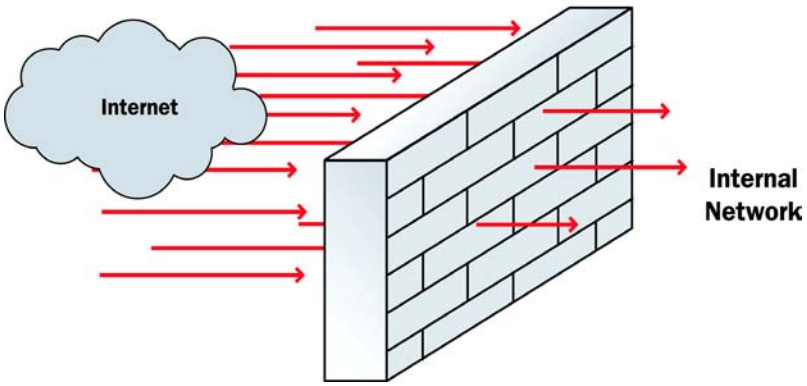
Most services are given a port number in the range from 0 to 1024, but possible port numbers range from 0 to 65535.

Firewalls

A firewall divides your internal network from the Internet to decrease risk from an external attack. The computers and networks on the Internet are the external network. The computers on the internal side of the firewall are the trusted computers. The figure below shows how a firewall divides the trusted computers from the Internet.



Firewalls use access policies to identify different types of information. They can also control which services or ports the protected computers can use on the Internet (outbound access). Many firewalls have sample security policies and users can select the policy that is best for them. With others, including the Firebox® X Edge e-Series, the user can customize these policies.



Firewalls can be in the form of hardware or software. Firewalls prevent unauthorized Internet users from private networks connected to the Internet. All messages that enter or go out of the trusted or

protected networks go through the firewall, which examines each message and denies those that do not match the security criteria.

The Firebox® X Edge and Your Network

The Firebox® X Edge controls all traffic between the external network and the trusted network. The Edge also includes an optional network. Use the optional network for computers with "mixed trust." For example, customers frequently use the optional network for their remote users or for public servers such as a web server or e-mail server. Your firewall can stop all suspicious traffic from the external network to your trusted and optional networks. The rules and policies that identify the suspicious traffic appear in "Configuring Firewall Settings" on page 77.

The Firebox X Edge e-Series is a firewall for small and remote offices. Some customers who purchase an Edge do not know much about computer networks or network security. There are wizards and many self-help tools for these customers. Advanced customers can use integration features to connect an Edge to a larger wide area network. The Edge connects to a cable modem, DSL modem, or ISDN router.

The Web-based user interface of the Firebox X Edge lets you manage your network safely. You can manage your Edge from different locations and at different times. It gives you more time and resources to use on other components of your business.

CHAPTER 2

Installing the Firebox X Edge e-Series

To install the WatchGuard® Firebox® X Edge e-Series in your network, you must complete these steps:

- Identify and record the TCP/IP properties for your Internet connection.
- Disable the HTTP proxy properties of your Web browser.
- Connect the Edge to your network.
- Connect your computer to the Edge.
- Use the Quick Setup Wizard to configure the Edge.
- Activate the LiveSecurity® Service.

Installation Requirements

To install the Firebox® X Edge e-Series, you must have:

- A computer with a 10/100BaseT Ethernet network interface card to configure the Edge.
- A Web browser. You can use Netscape 7.0 or later, Internet Explorer 6.0 or later, or an equivalent browser.
- The serial number of the Edge.

  You can find the serial number on the bottom of the device. Use the serial number to register the Edge.
- An Internet connection.

  The external network connection can be a cable or DSL modem with a 10/100BaseT port, an ISDN router, or a direct LAN connection. If you have problems with your Internet connection, call your ISP (Internet Service Provider) to correct the problem before you install the Firebox X Edge.

Package Contents

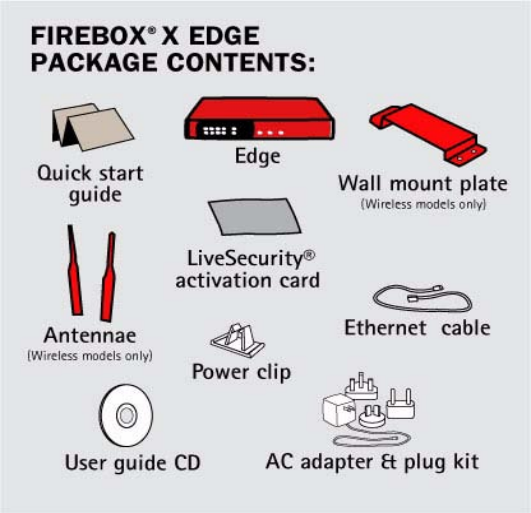
Make sure that the package for your Firebox® X Edge e-Series includes these items:

- *Firebox X Edge e-Series User Guide* on CD-ROM
- Firebox X Edge e-Series *Quick Start Guide*
- LiveSecurity® Service activation card
- Hardware warranty card

- AC power adapter (12 V/1.2A) with international plug kit.
- Power cable clip

Use this clip to attach the cable to the side of the Edge. This decreases the tension on the power cable.

- One straight-through Ethernet cable
- Wall mount plate (wireless models only)
- Two antennae (wireless models only)



Identifying Your Network Settings

To configure your Firebox® X Edge, you must know some information about your network. (For an overview of network basics, see "About Networks" on page 1.) Use this section to learn how to identify your network settings.

About network addressing

Speak with your ISP or corporate network administrator to learn how your computer gets its external IP address. Use the same method to connect to the Internet with the Firebox X Edge that you use with your computer. If you connect your computer directly to the Internet with a broadband connection, you can put the Edge between your computer and the Internet and use the network configuration from your computer to configure the Edge external interface. You can use a static IP address, DHCP, or PPPoE to configure the Edge external interface.

Your computer must have a Web browser. You use the Web browser to configure and manage the Firebox X Edge. Your computer must have an IP address on the same network as the Edge.

In the factory default configuration, the Firebox X Edge assigns your computer an IP address with DHCP (Dynamic Host Configuration Protocol). You can set your computer to use DHCP and you then can connect to the Edge to manage it. You can also give your computer a static IP address that is on the same network as the trusted IP address of the Edge. For more information, see "Setting Your Computer to Connect to the Edge" on page 17.

Static addresses, DHCP, and PPPoE

Your ISP gives you an IP address using one of these methods:

- Static: A *static IP address* is an IP address that always stays the same. If you have a Web server, FTP server, or other Internet resource that must have an address that cannot change, you can get a static IP address from your ISP. A static IP address is usually more expensive than a dynamic IP address, and some ISPs do not supply static IP addresses.
- DHCP: A *dynamic IP address* is an IP address that an ISP lets you use temporarily. ISPs use DHCP (Dynamic Host Configuration Protocol) to assign you a dynamic IP address. With DHCP, your computer does not always use the same IP address. Each time you connect to the ISP, a DHCP server assigns you an IP address. It could be the same IP address you had before, or it could be a new IP address. When you close an Internet connection that uses a dynamic IP address, the ISP can assign that IP address to a different customer.
- PPPoE: An ISP also can use PPPoE (Point-to-Point Protocol over Ethernet) to assign you an IP address. Usually, a PPPoE address is dynamic. You must have a user name and a password to use PPPoE.

The ISP also assigns a subnet mask (also known as the netmask) to a computer. A *subnet mask* divides a larger network into smaller networks. A subnet mask is a string of bits that "mask" one section of an IP address to show how many IP addresses can be on the smaller network.

Read your DSL or cable modem instructions or speak to your ISP to learn if you have a dynamic IP address or a static IP address.

TCP/IP properties

To learn about the properties of your network, look at the TCP/IP properties of your computer or any other computer on the network. You must have this information to install your Firebox X Edge. Use the table below to record the TCP/IP properties of your network. Use the procedures below to find the TCP/IP properties on your operating system.

Note

If your ISP assigns your computer an IP address that starts with 10, 192.168, or 172.16 to 172.31, then your ISP uses NAT (Network Address Translation) and your IP address is private. We recommend that you get a public IP address for your Firebox X Edge external IP address. If you use a private IP address, you can have problems with some features, such as VPN.

Your TCP/IP Properties

TCP/IP Property		Value
IP address		. . .
Subnet mask		. . .
Default gateway		. . .
DHCP enabled		Yes No
DNS server(s)	Primary	. . .
	Secondary	. . .

To find your TCP/IP properties, use the instructions for your computer operating system.

Finding your TCP/IP properties on Microsoft Windows 2000, Windows 2003, and Windows XP

1. Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.
   The Command Prompt window appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Record the values in the Table, "Your TCP/IP Properties," on page 11.

Finding your TCP/IP properties on Microsoft Windows NT

1. Click **Start** > **Programs** > **Command Prompt**.
   The Command Prompt window appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Record the values in the Table, "Your TCP/IP Properties," on page 11.

Finding your TCP/IP properties on Macintosh OS 9

1. Click the **Apple** menu > **Control Panels** > **TCP/IP**.
   The TCP/IP window appears.
2. Record the values in the Table, "Your TCP/IP Properties," on page 11.

Finding your TCP/IP properties on Macintosh OS X

1. Click the **Apple** menu > **System Preferences**, or select the icon from the Dock.
   The System Preferences window appears.
2. Click the **Network** icon.
   The Network preference pane appears.
3. From the **Show** drop-down list, select the network adapter you use to connect to the Internet.
4. Record the values in the Table, "Your TCP/IP Properties," on page 11.

Finding your TCP/IP properties on other operating systems (Unix, Linux)

1. Read your operating system guide to find the TCP/IP settings.
2. Record the values in the Table, "Your TCP/IP Properties," on page 11.

PPPoE settings

Many ISPs use Point to Point Protocol over Ethernet (PPPoE) because it is easy to use with a dial-up infrastructure. If your ISP uses PPPoE to assign IP addresses, you must get information about these settings. Use the table below to record PPPoE settings.

PPPoE Address Settings

PPPoE Setting	Value
Login name	
Domain (optional)	
Password	

Web Browser HTTP Proxy Settings

Many Web browsers are configured to use an HTTP proxy server to increase the download speed of web pages. To manage or configure the Firebox® X Edge e-Series, your browser must connect directly to the Edge. If you use an HTTP proxy server, you must temporarily disable the HTTP proxy setting in your browser. You can enable the HTTP proxy server setting in your browser after you set up the Edge.

Use these instructions to disable the HTTP proxy in Firefox, Mozilla, Netscape, or Internet Explorer. If you are using a different browser, use the browser Help system to find the necessary information. Many browsers automatically disable the HTTP proxy feature.

Disabling the HTTP proxy in Internet Explorer

1 Open Internet Explorer.

2 Click **Tools** > **Internet Options**.
The Internet Options window appears.

3 Click the **Connections** tab.

4 Click the **LAN Settings** button.
The Local Area Network (LAN) Settings window appears.

5 Clear the check box labeled **Use a proxy server for your LAN**.

6 Click **OK** two times.

Disabling the HTTP proxy in Firefox or Netscape

1 Open the browser software.

2 Click **Tools > Options**.
The Options window appears.

3 Click the **General** icon.
The General preference window appears.

4 Click the **Connection Settings** button.
The Connection Settings dialog box appears.

5 Make sure the **Direct Connection to the Internet** option is selected.

6 Click **OK** two times.

Disabling the HTTP proxy in Mozilla

1 Open the browser software.

2 Click **Edit > Preferences.**
The Preferences window appears.

3 Click the arrow adjacent to the **Advanced** label and select **Proxies**.
The Proxies preference window appears.
4 Make sure the **Direct Connection to the Internet** option is selected.
5 Click **OK**.

Web Browser Pop-up Blocking Settings

The Firebox® X Edge e-Series uses pop-up windows for many features, including the Quick Setup Wizard. If you block pop-up windows, you must disable this function when you connect to the Edge.

Use these instructions to disable the pop-up blocking option in Firefox, Mozilla, Netscape, or Internet Explorer. If you are using a different browser, use the browser Help system to find the necessary information.

Disabling the pop-up blocker in Internet Explorer

1 Open Internet Explorer.
2 Click **Tools** > **Pop-Up Blocker > Turn Off Pop-Up Blocker**.

Disabling the pop-up blocker in Firefox

1 Open the browser software.
2 Click **Tools > Options**.
The Options window appears.
3 If you are using the **Content** icon.
The Content or Site Controls preference window appears.
4 Make sure the **Block Popup Windows** option is not selected.
5 Click **OK**.

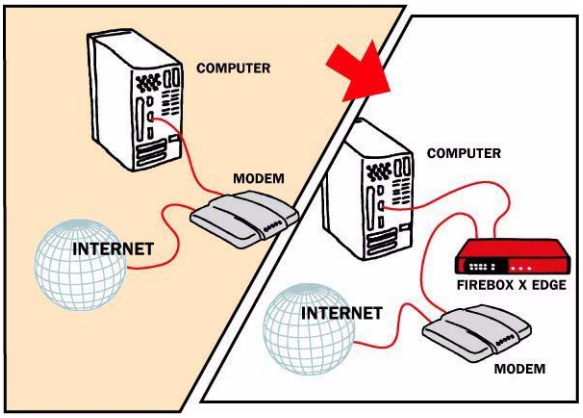
Disabling the pop-up blocker in Netscape

1 Open the browser software.
2 Click **Tools > Options**.
The Options window appears.
3 Click the **Site Controls** icon.
The Site Controls preference window appears.
4 Make sure the **Allow unrequested pop-up windows** option is not selected.
5 Click **OK**.

Disabling the pop-up blocker in Mozilla

1 Open the browser software.
2 Click **Edit > Preferences.**
The Preferences window appears.
3 Click the arrow adjacent to the **Privacy & Security** label and select **Popup Windows**.
The Popup Windows preference window appears.
4 Make sure the **Block unrequested popup windows** option is not selected.
5 Click **OK**.

Connecting the Firebox X Edge

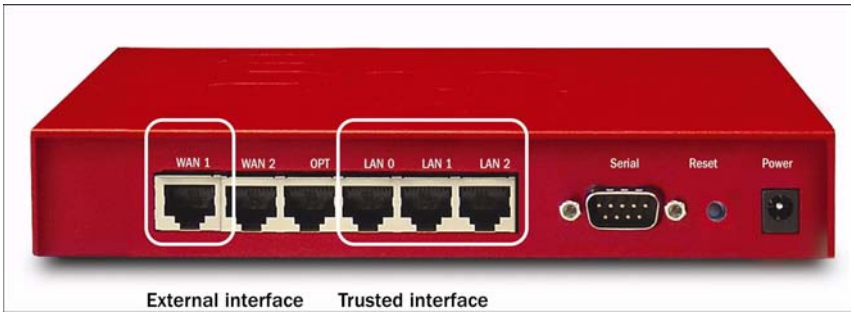


Use this procedure to connect Ethernet and power cables to your Firebox® X Edge:

1 Shut down your computer.

2 If you use a DSL or cable modem to connect to the Internet, disconnect its power supply.

3 Find the Ethernet cable between the modem and your computer. Disconnect this cable from your computer and connect it to the Edge external interface (labeled WAN 1).



4 Find the Ethernet cable supplied with your Edge. Connect this cable to a trusted interface (LAN0-LAN2) on the Edge. Connect the other end of this cable to the Ethernet interface of your computer.

5 If you use a DSL or cable modem, connect its power supply.

6 Find the AC adapter supplied with your Edge. Connect the AC adapter to the Edge and to a power source.
The Edge power indicator light comes on, then the WAN indicator lights flash and then come on.

Note

Use only the supplied AC adapter for the Firebox X Edge.

Connecting the Edge to more than four devices

The Firebox X Edge e-Series has three Ethernet ports (LAN0-LAN2) for the trusted network, and one Ethernet port (OPT) for the optional network. You can connect devices directly to the Edge, or use a hub or switch to connect more than four devices. The number of devices that can connect to the external

network is limited by the number of session licenses available. See the subsequent section, "About session licenses" for more information.

To connect more than four devices to the Edge, you must have:

- An Ethernet 10/100Base TX hub or switch
- A straight-through Ethernet cable, with RJ-45 connectors, for each computer
- A straight-through Ethernet cable to connect each hub to the Firebox X Edge

To connect more devices to the Firebox X Edge:

1 Shut down your computer.

2 If you use a DSL or cable modem to connect to the Internet, disconnect its power supply.

3 Disconnect the Ethernet cable that comes from your DSL modem, cable modem, or other Internet connection to your computer. Connect the Ethernet cable to the WAN1 port on the Firebox X Edge.
The Firebox X Edge is connected directly to the modem or other Internet connection.

4 Connect one end of the straight-through Ethernet cable supplied with your Firebox X Edge to one of the four Ethernet ports on the Edge. Connect the other end to the uplink port of the Ethernet hub or switch.
The Firebox X Edge is connected to the Internet and your Ethernet hub or switch.

5 Connect an Ethernet cable between each computer and one of the ports on the Ethernet hub, and make sure the link lights are lit on the devices when they are turned on.

6 If you connect to the Internet through a DSL modem or cable modem, connect the power supply to this device. The indicator lights flash and then stop.

7 Attach the AC adapter to the Firebox X Edge. Connect the AC adapter to a power supply.

About session licenses

Any device connected to the trusted or optional network on the Firebox X Edge can connect to other devices on the trusted or optional networks. The maximum number of devices that can connect to the external network from the trusted or optional networks is set by model. For example, if an Edge has a 15-session license, 15 devices from the trusted network can connect to the Internet. You can upgrade the session license on your Edge to allow more devices to connect.

When a device on the trusted or optional network makes a connection to the external network, one session is used. A device can have more than one connection to the external network without using more sessions.

The Edge releases a session when any of these things happen:

- If user authentication is necessary for external network connections and no data is sent or received, the Edge releases the session after the idle time-out limit set for that account.
- If user authentication is necessary for external network connections, the Edge releases the session after the maximum time-out limit set for that account.
- If user authentication is necessary for external network connections, the Edge releases the session when the user logs out and then closes all browser windows.
- If the Edge administrator uses the Firebox Users page to stop a session, the Edge releases that session.
- If the Automatic Session Termination time limit expires, all sessions are released.
- If the Edge restarts, all sessions are released.

For more information, see the FAQ:

www.watchguard.com/support/AdvancedFaqs/edge_seatlicense.asp

License upgrades are available from your reseller or from the WatchGuard® Web site:

http://www.watchguard.com/products/purchaseoptions.asp

Setting Your Computer to Connect to the Edge

Before you can use the Quick Setup Wizard, you must configure your computer to connect to the Firebox® X Edge. You can set your network interface card to use a static IP address, or use DHCP to get an IP address automatically.

If your computer gets its address from DHCP

This procedure configures a computer with the Windows XP operating system to use DHCP. If your computer does not use Windows XP, read the operating system help for instructions on how to set your computer to use DHCP.

1. Click **Start > Control Panel**.
   The Control Panel window appears.
2. Double-click the **Network Connections** icon.
3. Double-click the **Local Area Connection** icon.
   The Local Area Connection Status window appears.
4. Click the **Properties** button.
   The Local Area Connection Properties window appears.
5. Double-click the **Internet Protocol (TCP/IP)** list item.
   The Internet Protocol (TCP/IP) Properties dialog box appears.
6. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** options.
7. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
8. Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Local Area Connection Status**, **Network Connections,** and **Control Panel** windows.
   Your computer is ready to connect to the Firebox X Edge.
9. When the Edge is ready, start your Internet browser.
10. Type `https://192.168.111.1/` into the URL entry field of your browser and press **Enter**. If you are asked to accept a security certificate, click **OK**.
    The Quick Setup Wizard starts.
11. Run the Quick Setup Wizard.

If your computer has a static IP address

This procedure configures a computer with the Windows XP operating system to use a static IP address. If your computer does not use Windows XP, read the operating system help for instructions on how to set your computer to use a static IP address.

You must select an IP address on the same subnet as the trusted network.

1 Click **Start > Control Panel**.
The Control Panel window appears.

2 Double-click the **Network Connections** icon.

3 Double-click the **Local Area Connection** icon.
The Local Area Connection Status window appears.

4 Click the **Properties** button.
The Local Area Connection Properties window appears.

5 Double-click the **Internet Protocol (TCP/IP)** list item.
The Internet Protocol (TCP/IP) Properties dialog box appears.

6 Select the **Use the following IP address** option.

7 In the **IP address** field, type an IP address on the same network as the Edge trusted interface. We recommend 192.168.111.2.
The default trusted interface network is 192.168.111.0/24. The last number can be between 2 and 254.

8 In the **Subnet Mask** field, type `255.255.255.0`.

9 In the **Default Gateway** field, type the IP address of the Edge trusted interface.
The default Edge trusted interface address is 192.168.111.1.

10 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.

11 Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Local Area Connection Status**, **Network Connections** and **Control Panel** windows.
Your computer is ready to connect to the Firebox X Edge.

12 When the Edge is ready, start your Internet browser.

13 Type `https://192.168.111.1/` into the URL entry field of your browser and press **Enter**. If you are asked to accept a security certificate, click **OK**.
The Quick Setup Wizard starts.

14 Use the Quick Setup Wizard, as shown in the subsequent section.

Using the Quick Setup Wizard

The Quick Setup Wizard starts after you type **https://192.168.111.1** into the URL or address field of your Internet browser. If your browser blocks pop-up windows, you must disable that function to complete the Quick Setup Wizard. You must use the wizard to configure the Ethernet interfaces. You can change the configuration of the interfaces after you use the wizard.

The Quick Setup Wizard includes this set of dialog boxes. Some dialog boxes only appear based on the configuration method you select:

Welcome
The first screen tells you about the wizard.

Configure the External Interface of your Firebox
Select the method your ISP uses to assign your IP address.

Configure the External Interface for DHCP
Type your DHCP identification as supplied by your ISP.

Configure the External Interface for PPPoE

Type your PPPoE information as supplied by your ISP.

Configure the External Interface with a static IP address

Type your static IP address information as supplied by your ISP.

Configure the Trusted Interface of the Firebox

Type the IP address of the trusted interface.

Set the User Name and Passphrase

Enter a user name and passphrase for the administrator account for the Edge.

Set the Wireless Region

(For wireless models only.) Type the country or region in which the Firebox® X Edge e-Series Wireless is being used. The country or region cannot be changed after it is set.

Set the Time Zone

Use this screen to set the time zone the Firebox X Edge is operating in.

The Quick Setup Wizard is complete

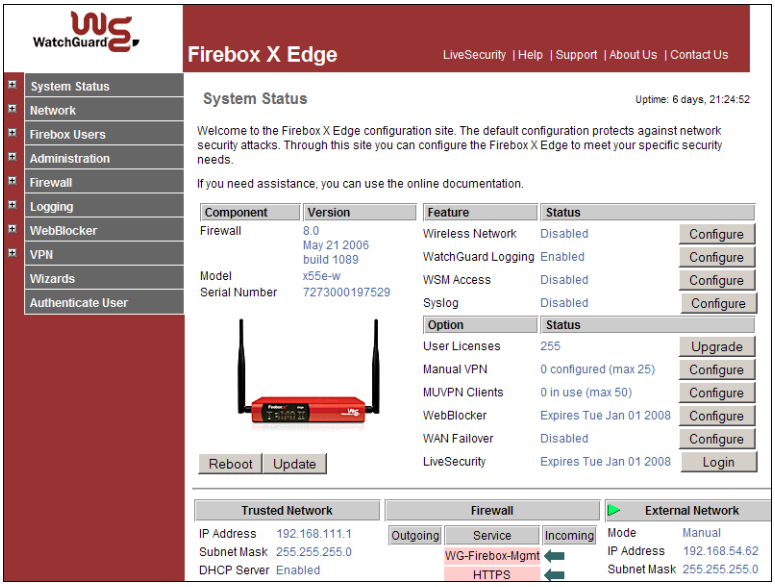
The Quick Setup Wizard shows a link to the WatchGuard web site to register your product. After you complete the wizard, the Firebox X Edge restarts.

Note

If you change the IP address of the trusted interface, you must change your network settings so that your IP address matches the subnet of the trusted network before you connect to the Firebox X Edge again. If you use DHCP, restart your computer. If you use static addressing, see "If your computer has a static IP address" on page 18.

The System Status page

The System Status page appears on the screen. You can configure more features of your Edge from this page.



Registering and Activating LiveSecurity Service

After you install the Firebox® X Edge e-Series, you can register the Edge and activate your LiveSecurity® service subscription. The LiveSecurity service gives you threat alert notifications, security advice, virus protection information, software updates, technical support by Web or telephone, and access to online help resources and the WatchGuard® user forum.

You must have a subscription to the LiveSecurity service to install upgrades that you purchase. To install an upgrade, log in to the LiveSecurity service and type your upgrade key. You then receive a feature key to activate the feature on your Firebox X Edge.

To register, find the serial number of your Firebox X Edge. The Edge serial number is printed on the bottom of the device. Record your serial number in the table below and complete these steps:

1 Register your Firebox X Edge e-Series with the LiveSecurity Service at the WatchGuard web site:
http://www.watchguard.com/activate

Note

To activate the LiveSecurity Service, your browser must have JavaScript enabled.

2 If you are registered at the WatchGuard web site, type your user name and password. If you are not registered, you must create a user account. To do this, follow the instructions on the web site.

3 Record your LiveSecurity service user profile information in the table below. Keep this information confidential.

WatchGuard LiveSecurity Service User Profile

User name:	
Password:	
Serial number:	

4 If a model upgrade key is included with your model, activate it at:
http://www.watchguard.com/upgrade

5 Select your product and follow the instructions for product activation. At this time you can configure your Edge.

CHAPTER 3

Navigating the Firebox X Edge e-Series Configuration Pages

After you connect the WatchGuard® Firebox® X Edge e-Series to your network, you must configure the Edge. You can create firewall rules to enforce the security requirements of your company. You also can use the Edge configuration pages to create an account, look at network statistics, and see the configuration of the Edge.

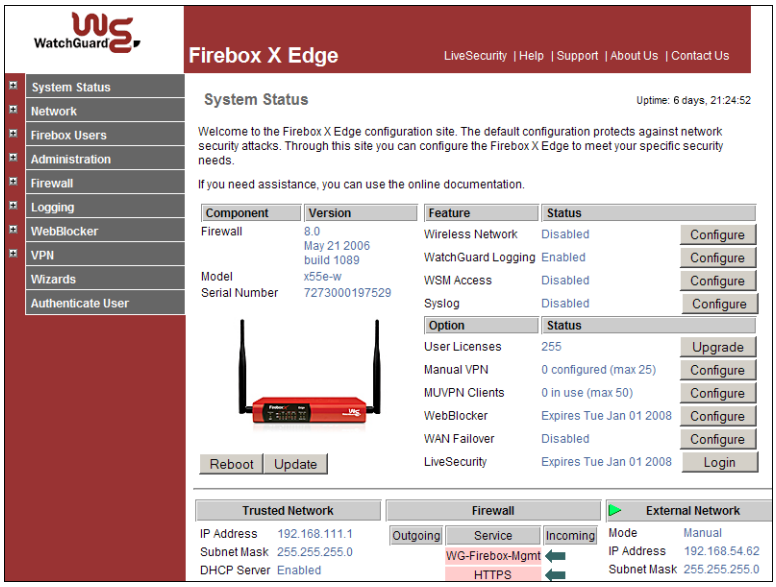
Read this chapter to find basic information about the Firebox X Edge configuration pages. There are sections in subsequent chapters that have more advanced procedures. This chapter contains links to subsequent sections.

Note

You must complete the Quick Setup Wizard before you can view the Firebox X Edge configuration pages.. For more information, see "Using the Quick Setup Wizard" on page 18. Also, your network administrator must configure your user account to see and change the configuration pages. For more information on user accounts, see "Managing Users and Groups" on page 107.

Navigating the Configuration Pages

All configuration procedures for the Firebox® X Edge e-Series use the configuration pages. The System Status page appears when you connect to the Edge.



In this User Guide, most procedures start with this step:

"To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface. The default URL is: https://192.168.111.1."

This opens your Firebox system configuration pages. You can change the IP address of the trusted network from 192.168.111.1 to a different IP address if necessary. For more information, see "Configuring the Trusted Network" on page 50.

For example:

1 Start your web browser.

2 Click **File** > **Open**, type `https://192.168.111.1` in the **Open** text box and click **OK**.
You also can type `https://192.168.111.1` directly into the address or location bar and press Enter.

3 When a security certificate notification appears, click Yes.
This warning will appear each time you connect to the Firebox X Edge using HTTPS.

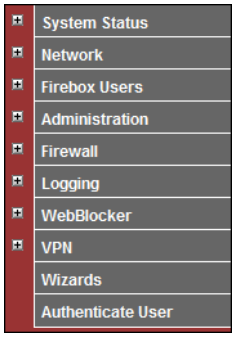
4 Enter your user name and password to authenticate.
The System Status page appears.

Note

If necessary, you can connect to the web server on the Firebox X Edge using HTTP instead of HTTPS. HTTP is less secure, because any information you send to the Firebox is unencrypted. We recommend that you always use HTTPS to configure the Firebox X Edge.

Using the navigation bar

On the left side of the System Status page is the navigation bar you use to get to other Firebox X Edge configuration pages.



To see the primary page for each feature, click the menu item on the navigation bar. For example, to see how logging is configured for the Firebox X Edge and to see the current event log, click **Logging**.

Each menu item contains secondary menus that you use to configure the properties of that feature. To see these secondary menus, click the plus sign (+) to the left of the menu item. For example, if you click the plus sign adjacent to **WebBlocker**, these secondary menu items appear: **Settings, Profiles, Allowed Sites,** and **Denied Sites**.

This User Guide uses an arrow (>) symbol to show menu items that you expand or click. The menu names are in **bold**. For example, the command to open the Denied Sites page appears in the text as **WebBlocker > Denied Sites.**

Configuration Overview

You use the Firebox® X Edge e-Series system configuration pages to set up your Edge and protect your network. This section gives an introduction to each category of pages, and tells you where to find more information about each category in the User Guide.

System Status page

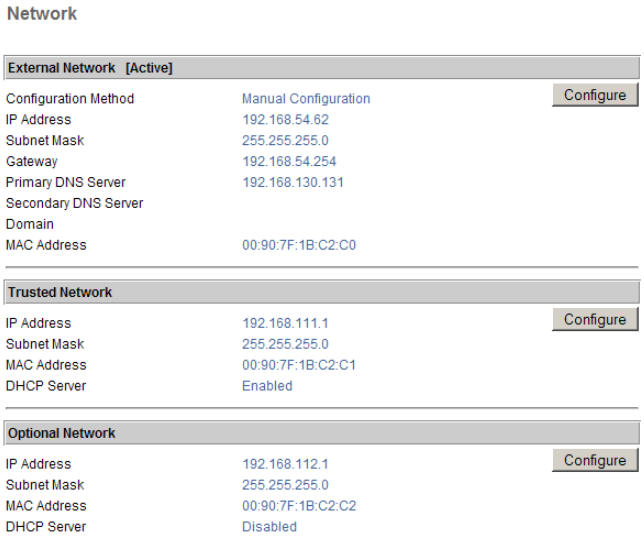
The System Status page is the primary configuration page of the Firebox X Edge e-Series. The center panel of the page shows information about the current settings. It also contains the buttons you use to change these settings. You can see more information about each property in subsequent chapters.

The information on this page includes:

- Edge components and their current versions
- The serial number of the device
- The status of key Edge features
- The status of upgrade options
- Network configuration information
- Which external network (external or failover) is active. A green triangle appears adjacent to the active network.
- Firewall configuration information
- Buttons to restart or update the Edge

Network page

The Network page shows the current configuration of each interface and network route. Adjacent to each section is a button you can use to change configurations and to see network statistics. For more information, see “Changing Your Network Settings” on page 45



The **Network** menu contains links to these pages:

External
: Configure the Edge external network interface, or how the Edge connects to the Internet and other networks.

Trusted
: Configure the Edge trusted network interface, or how the Edge gives IP addresses to devices on the trusted network

Optional
: Configure the Edge optional network interface, or how the Edge gives IP addresses to devices on the optional network.

Traffic Control
: Create filters that send important network traffic first.

Wireless (802.11g)
: Set up and configure the wireless network (wireless models only).

WAN Failover
: Configure a redundant network connection for the external interface.

Dynamic DNS
: Register the external IP address of the Edge when using a dynamic DNS (Domain Name Server) service.

BIDS
: Connection settings for Telstra customers.

Routes
: Create a static route to a device on the trusted or optional network from the external interface.

Firebox Users page

The **Firebox Users** page shows statistics on active sessions and local user accounts. It also has buttons to close current sessions and to add, edit, and delete user accounts.

This page also shows the MUVPN client configuration files that you can download. For more information, see Chapter 9 "Managing Users and Groups."

The **Firebox Users** menu contains links to these pages:

Settings
Use this page to set the properties that apply to all Edge users.

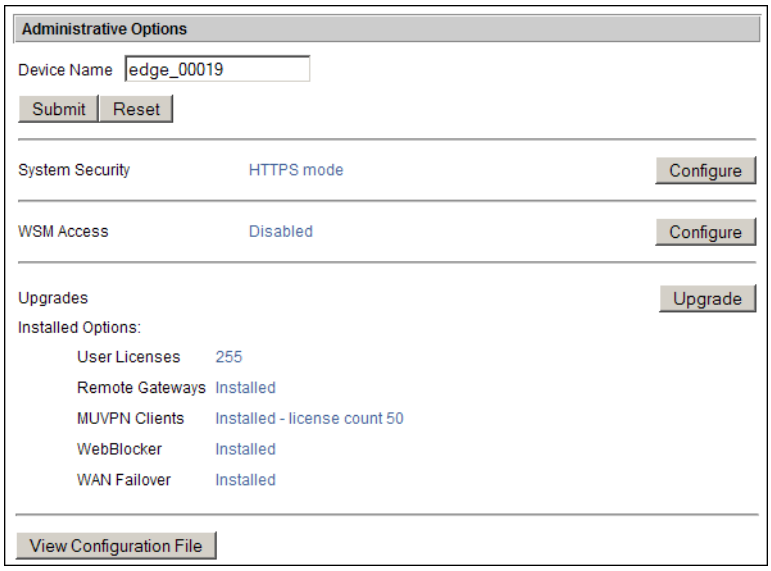
New User
Create one or more user accounts and set the types of network traffic that users can send and receive.

New Group
Use this page to add a user group.

Trusted Hosts
Use this page to add the IP addresses of users who are exempt from the configured authentication and WebBlocker rules.

Administration page

The Administration page shows if the Firebox X Edge uses HTTP or HTTPS for its configuration pages, if the Edge is configured as a managed Firebox client, and which feature upgrades are enabled. It has buttons to change configurations, add upgrades, and see the configuration file. You can also change the name of the Firebox. For more information, see Chapter 4, "Configuration and Management Basics."



The **Administration** menu contains links to these pages:

System Security
Select HTTP or HTTPS for administrative access.

WSM Access
Enable remote management of the Firebox X Edge through the WatchGuard® Management Server.

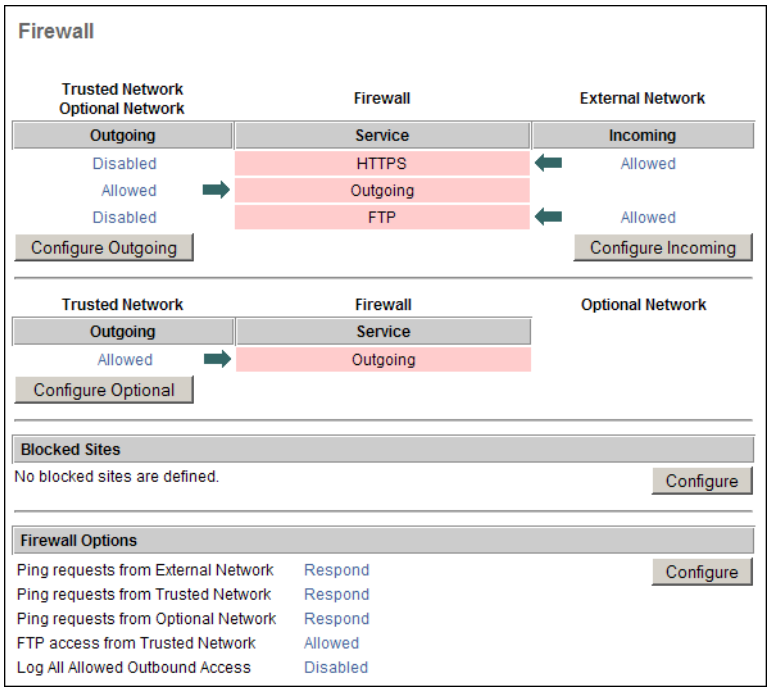
Update
Update the Firebox X Edge e-Series firmware.

Upgrade
Activate your Edge upgrade options.

View Configuration
Shows the Edge configuration file as text.

Firewall page

The Firewall page shows incoming and outgoing services, blocked Web sites, and other firewall settings. This page also has buttons to change these settings. For more information, see Chapter 7, "Configuring Firewall Settings."



The **Firewall** menu contains links to these pages:

Incoming
Make one or more security services for incoming traffic to the trusted or optional networks.

Outgoing
Make one or more security services for outgoing traffic to the external network.

Optional
Make one or more security services for outgoing traffic from the trusted to the optional network.

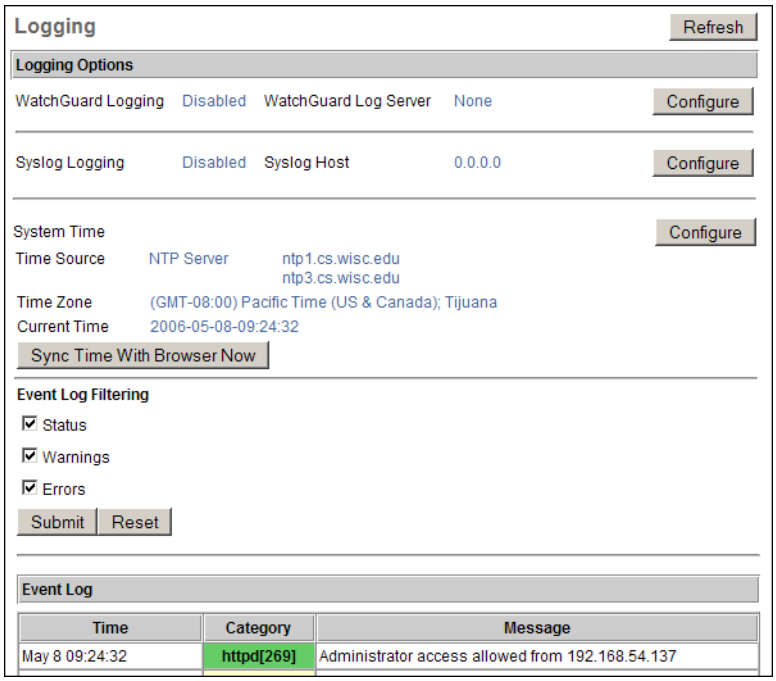
NAT
Define settings for automatic address translation and for 1-to-1 address translation.

Blocked Sites
Prevent access to specified network addresses on the external interface.

Firewall Options
Customize your security policy.

Logging page

The Logging page shows the current event log, the status of the Log Server and syslog logging, and the system time. It also has buttons to change these properties and to set your system time to the same value as your local computer. For more information, see "Configuring Logging and System Time" on page 103.



The **Logging** menu contains links to these pages:

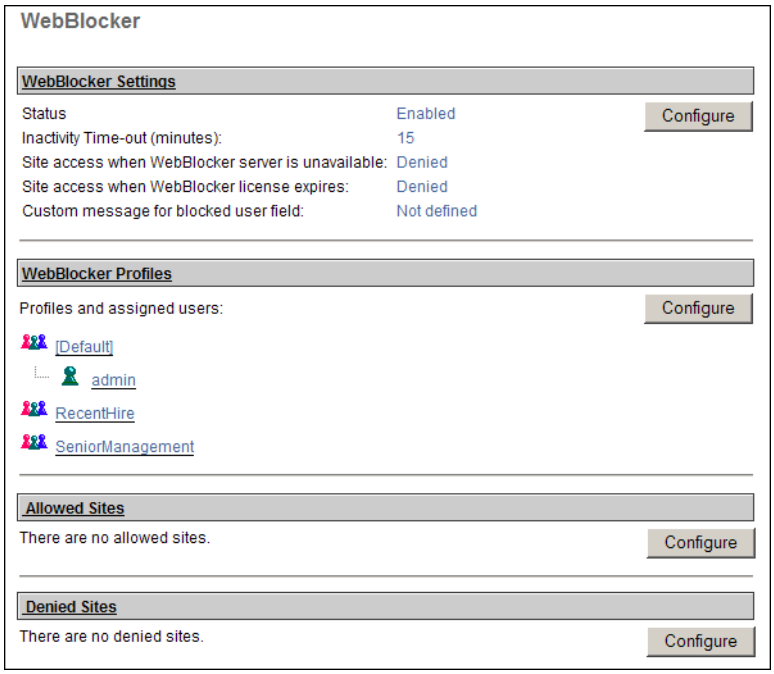
WatchGuard Logging
Configure the WatchGuard® Log Server to accept log messages from your Firebox X Edge.

Syslog Log
Configure the Edge to send log messages to a syslog host.

System Time
Set the time zone and if your Edge uses daylight saving time.

WebBlocker page

The WebBlocker page shows the WebBlocker settings, profiles, allowed sites, and denied sites. It also has buttons to change the current settings. For more information, see Chapter 10, "Configuring WebBlocker."



The **WebBlocker** menu contains links to these pages:

Settings
: Configure the WebBlocker settings for all users.

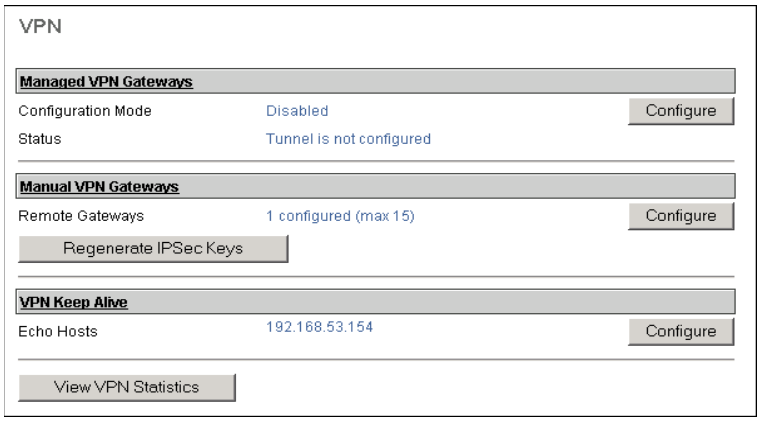
Profiles
: Create sets of restrictions and apply them to groups of Firebox X Edge users.

Allowed Sites
: Make a list of Web sites that you can browse to when WebBlocker properties block the Web site.

Denied Sites
: Make a list of Web sites that you cannot browse to when WebBlocker settings allow the Web site.

VPN page

The VPN page shows information on managed VPN gateways, manual VPN gateways, echo hosts, and buttons to change the configuration of VPN tunnels. It also has a button for you to see statistics on active tunnels. You can add the Firebox® X Edge e-Series to a Watchguard System Manager VPN network with the WSM Access page in Administration. For more information, see "Configuring Virtual Private Networks" on page 135.



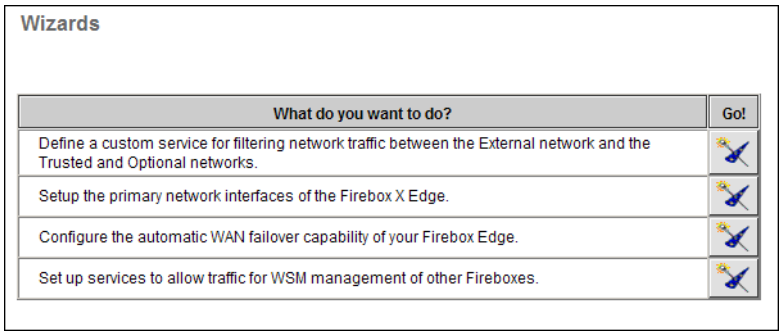
The **VPN** menu contains links to these pages:

Manual VPNs
Make a VPN tunnel to an IPSec compliant device, such as a second Firebox X Edge.

VPN Keep Alive
Keep a VPN tunnel open when no regular network traffic goes through it.

Wizards page

The Wizards page shows the wizards you can use to help you set up Firebox X Edge features. Each wizard launches a new window to help you configure the Edge settings.


Wizards
What do you want to do?
Go!
Define a custom service for filtering network traffic between the External network and the Trusted and Optional networks.
Setup the primary network interfaces of the Firebox X Edge.
Configure the automatic WAN failover capability of your Firebox Edge.
Set up services to allow traffic for WSM management of other Fireboxes.

If a wizard is not available, it is not shown on the Wizards page. Some of the wizards include:

Service Configuration Wizard
Create a rule to filter network traffic between interfaces. For more information, see “About custom services for incoming traffic” on page 80.

Network Interface Wizard
Configure the Edge interfaces. For more information, see “Using the Network Setup Wizard” on page 45.

Wireless Network Wizard (wireless models only)
Set up the wireless interface. For more information, see Chapter 6, “Setting up the Firebox X Edge Wireless.”

WAN Failover Setup Wizard

Set up the failover network. For more information, see "Enabling the WAN Failover Option" on page 60.

CHAPTER 4

Configuration and Management Basics

After your Firebox® X Edge e-Series is installed on your network and operating with a basic configuration file, you can start to add custom configuration settings to meet the needs of your organization. This chapter shows you how to do some basic management and maintenance tasks.

These basic configuration tasks include:

- Restore the Firebox X Edge to factory default settings
- Restart the Edge
- Set the system time
- Set management preferences
- Enable remote management on the Edge
- Update the firmware
- Activate upgrade options

Factory Default Settings

The term *factory default settings* refers to the configuration on the Firebox® X Edge when you first receive it before you make changes to the configuration file. The default network and configuration properties for the Edge are:

Trusted network

- The default IP address for the trusted network is 192.168.111.1. The subnet mask for the trusted network is 255.255.255.0.
- The Firebox X Edge is configured to give IP addresses to computers on the trusted network through DHCP. You also can give static addresses to computers in the trusted network with IP addresses in the 192.168.111.2 to 192.168.111.254 range.

External network

- The external network properties use DHCP.

Optional network

- The optional network is disabled.

Firewall settings

- All incoming services are denied.
- The outgoing service allows all outgoing traffic.
- Ping requests received on the external network are denied.

System Security

- The Firebox X Edge e-Series administrator account is set to the default user name of "admin" and the default passphrase of "admin." When you connect to the Edge, the Quick Setup Wizard includes a dialog box for you to set the administrator account user name and passphrase. After you complete the Quick Setup Wizard, you must use the user name and password that you selected to see the configuration pages.
- The Firebox X Edge is set up for local management only.

WebBlocker

- The WebBlocker feature is disabled and no properties are configured.

Upgrade Options

- Upgrade options are always available. You must type the license keys into the configuration page to activate upgrade options. If you restore the Firebox X Edge to its factory default settings, you do not have to type the license keys again.

Restoring the Firebox to the factory default settings

If you cannot correct a configuration problem and must "start over," you can go back to the factory default settings. For example, if you do not know the administrator account passphrase or a power interruption causes damage to the Firebox X Edge firmware, you can restore the Edge to the factory default settings.

Use these steps to set the Firebox X Edge e-Series to the factory default settings:

1 Disconnect the power supply.

2 Hold down the **Reset** button on the rear side of the Edge.

3 Connect the power supply while you continue to hold down the **Reset** button.

4 Continue to hold down the button until the yellow Attn light stays on. This shows you that the Edge was successfully restored to the factory default settings.

Note

Do not try to connect to the Edge at this time. Restart the Edge one more time, as the subsequent steps show. If you do not restart the Edge one more time, when you try to connect to the Edge you will see a web page that shows the message, "Your WatchGuard® Firebox X Edge is running from a backup copy of firmware." You also could see this message if the reset button is stuck in the depressed position. If you continue to see this page, check the reset button, and restart the Edge again.

5 Disconnect the power supply.

6 Connect the power supply again.
The Power Indicator is on and your Edge is reset.

Restarting the Firebox

You can restart the Firebox® X Edge e-Series from a computer on the trusted network. You also can restart the Edge from a computer on the Internet connected to the Edge external interface after you enable external access for this function.

The Firebox X Edge restart cycle is approximately one minute. During the restart cycle, the mode indicator on the front of the Edge turns off and then turns on again.

Local restart

You can locally restart the Firebox X Edge e-Series using one of two methods: use the web browser, or disconnect the power supply.

Using the web browser

1 To connect to the System Status page, type `https://` in the browser address bar, and then the IP address of the Firebox X Edge trusted network interface.
The default URL is: https://192.168.111.1

2 Click **Reboot**.

Disconnecting the power supply

Disconnect the Firebox X Edge power supply. Wait for a minimum of 10 seconds, and then connect the power supply.

Remote reboot

You must configure the Firebox X Edge e-Series to allow incoming HTTPS traffic to the Edge trusted interface IP address if the computer is not on the trusted interface. For more information on how to configure the Edge to receive incoming traffic, see "Configuring Incoming Services" on page 78. After HTTPS traffic is allowed, you can remotely manage your Edge using your browser from a trusted IP address. To do a remote reboot:

1 To connect to the System Status page, type `https://` in the browser address bar, and then the IP address of the Firebox X Edge external interface.

2 Click **Reboot**.

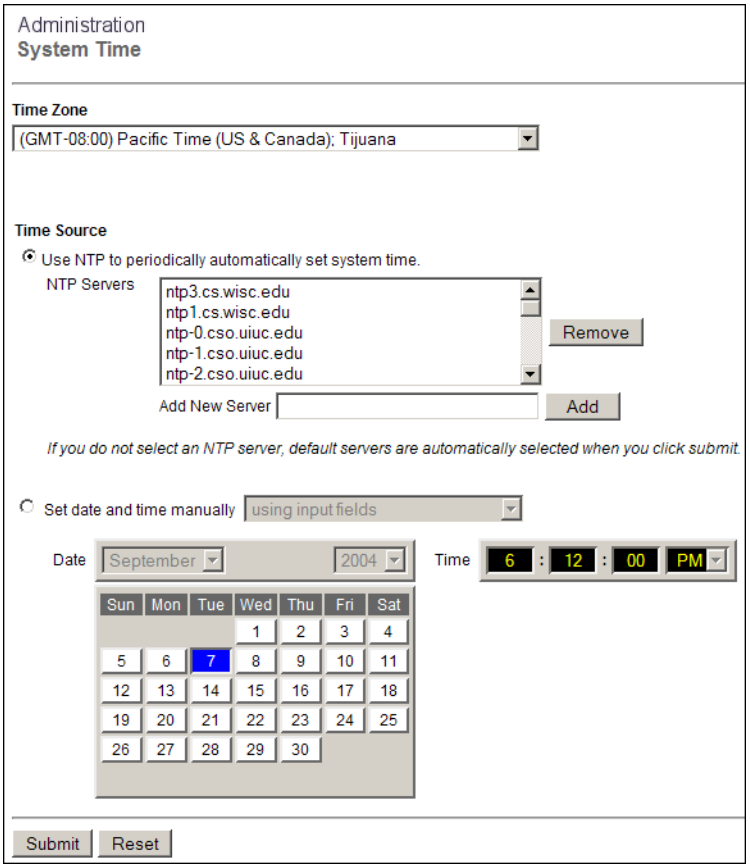
Setting the System Time

For each log message, the Firebox® X Edge e-Series records the time from its system clock. The Edge uses NTP to get the correct time automatically. You can change the NTP server that the Edge uses, or you can set the system time manually.

To set the system time:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **Logging** > **System Time**.
The System Time page appears.



3 Select the time zone from the drop-down list.

4 To set the system time automatically, select the **Use NTP to periodically automatically set system time** option. To set the time manually, select the **Set date and time manually** option.
If you set the system time manually, skip to step 6.

5 If you set the system time automatically, the Firebox X Edge gets the current time from the selected server in the NTP Servers list. If a server is not available, the Edge uses the subsequent server.
- To add a time server, type the server name in the **Add New Server** field and click **Add**.
- To remove a time server, select the server from the NTP Servers list and click **Remove**.
- Click a server to select it as the default time server.
To save your changes, skip to step 8.

6 If you set the system time manually, you must set the date and time separately.
- Select the month from the first drop-down list.
- Select the year from the second drop-down list.
- Click the button with the number that is today's date.

7 To the right of the date, set the time.
- Type the hours in the first field.
- Type the minutes in the second field.
- Type the seconds in the third field.
- Select **AM** or **PM** from the drop-down list.

8 Click **Submit**.

Selecting HTTP or HTTPS for Management

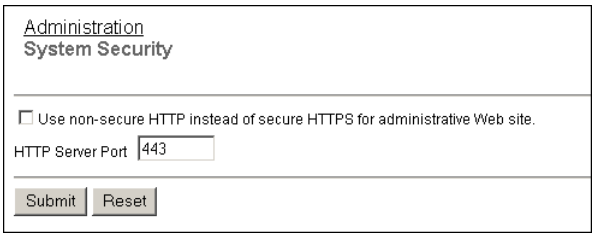
HTTP (Hypertext Transfer Protocol) is the "language" used to move files (text, graphic images, and multi-media files) on the Internet. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is a more secure version of HTTP. When using HTTPS, the Web server and your browser encrypt and decrypt the information you transmit. The Firebox® X Edge e-Series uses HTTPS by default, for better security.

To make the Firebox X Edge configuration pages appear more quickly, you can use HTTP. Using HTTP is less secure. When you use HTTP, all configuration changes are sent to the Edge from your computer in clear text. We recommend that you always use HTTPS to configure your Edge. You must connect to the Firebox X Edge using HTTPS one time before you can connect using HTTP.

Follow these instructions to use HTTP instead of HTTPS:

1 Type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Administration** > **System Security**.
The System Security page appears.



3 Select the **Use non-secure HTTP instead of secure HTTPS for administrative Web site** check box.
You will see a warning to make sure you change the HTTP server port to its default port of 80. To connect to the Firebox X Edge, you must use the same port in your browser as the HTTP server port on the Edge.

4 Click **Submit**.

If you select this check box, type `http://` in the browser address bar instead of the default `https://` to see the configuration pages.

Changing the HTTP Server Port

To see the Firebox® X Edge e-Series configuration pages, or for a user to authenticate to the Edge, the browser must connect on the same port as the Edge HTTP server. Because HTTPS uses TCP port 443 (HTTP uses TCP port 80), the default HTTP server port for the Edge is 443.

To change the port that you use to connect to the Firebox X Edge, type the new value in the **HTTP Server Port** field in the System Security configuration page shown above.

Note

After you change the HTTP server port, you must type the port when you connect to the Firebox X Edge. For example, if you change the HTTP server port to 880, you would type: http://192.168.111.1:880/

For more information on using HTTP or HTTPS with the Firebox X Edge and changing the HTTP Server Port, see this FAQ:

https://www.watchguard.com/support/advancedfaqs/edge_httpserverport.asp

You must log in to your LiveSecurity account to see this FAQ.

Setting up WatchGuard System Manager Access

Use the WatchGuard® System Manager (WSM) Access page to enable remote management by WatchGuard System Manager.

- With WatchGuard System Manager 8.3.1 and above, you can manage policies, updates, and VPNs for many Edge devices from one location.
- With WatchGuard System Manager v7.3 or below, you can use VPN Manager to create managed VPN tunnels between a Firebox® X Edge and a different WatchGuard Firebox.

Rename the Firebox X Edge e-Series

When you use WatchGuard System Manager to manage many different Edge devices, you can rename the Firebox X Edge e-Series so that it shows a unique name in WatchGuard System Manager.

To rename your Edge:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Administration**.
The Administration page appears.

3 Type the name of your Firebox X Edge e-Series in the **Device Name** field.

4 Click **Submit**.
The Firebox X Edge e-Series will use this name in the WatchGuard System Manager.

Enable remote management with WSM v8.3.1 or higher

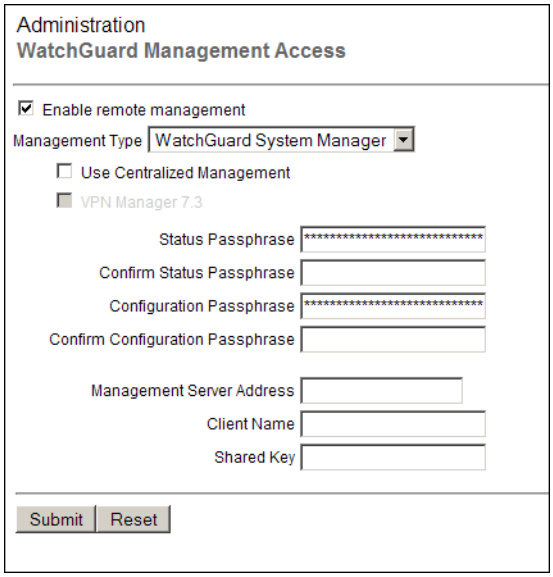
Follow these instructions to configure remote access from WatchGuard System Manager v8.2 or above. These versions of WatchGuard System Manager allow centralized management of Firebox X Edge devices.

Note

WSM v8.2 or later can manage Firebox X Edge (version 7.5) devices.
To manage Firebox X Edge e-Series (version 8.0) devices, you must use WSM v8.3.1.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Administration** >**WSM Access**.
The WatchGuard System Manager Access page appears.



3 Select the **Enable remote management** check box.

4 From the **Management Type** drop-down list, select WatchGuard Management System.

5 To enable centralized Edge management through WatchGuard System Manager, click the **Use Centralized Management** check box.

When the Firebox X Edge is under centralized management, access to the Edge configuration pages is set to read-only. The only exception is access to the WSM Access configuration page. If you disable the remote management feature, you get read-write access to Edge configuration again.

Do not select the **Use Centralized Management** check box if you are using WatchGuard System Manager only to manage VPN tunnels.

6 Type a status passphrase for your Firebox X Edge and then type it again to confirm.

7 Type a configuration passphrase for your Firebox X Edge and then type it again to confirm.

Note

These passphrases must match the passphrases you use when you add the device to WatchGuard System Manager, or the connection will fail.

8 In the **Management Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox protecting the Management Server.
The Firebox protecting the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. No special configuration is required for this to occur.

9 Type the **Client Name** to give to your Firebox X Edge.
This is the name used to identify the Edge in the Management Server.

10 Type the **Shared Key**.
The shared key is used to encrypt the connection between the Management Server and the Firebox X Edge. This shared key must be the same on the Edge and the Management Server. Get the shared key from your VPN administrator.

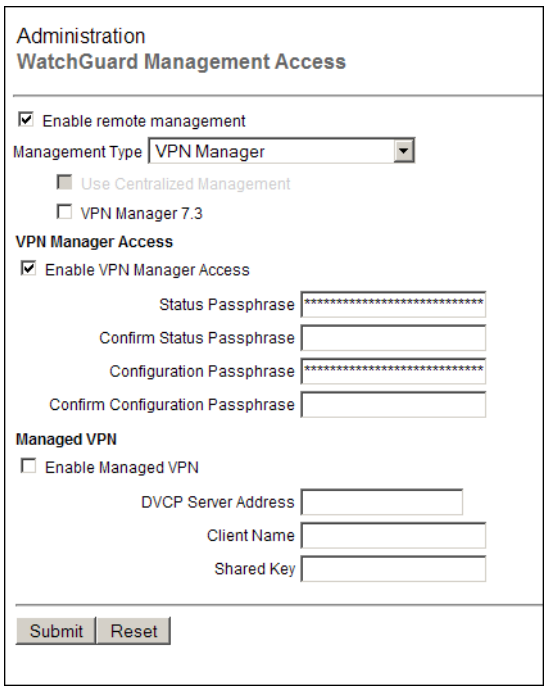
11 Click **Submit**.

Enable remote management with WFS v7.3 or earlier

Follow these instructions to configure remote access from WatchGuard Firebox System v7.3 or earlier. These versions of WatchGuard Firebox System use VPN Manager where the Firebox is the DVCP Server.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Administration** >**WSM Access**.
The WatchGuard System Manager Access page appears.



3 Select the **Enable remote management** check box.

4 From the **Management Type** drop-down list, select **VPN Manager**.

5 If you use VPN Manager 7.3, click the **VPN Manager 7.3** check box.

6 Click the **Enable VPN Manager Access** check box to allow VPN Manager to connect to the Firebox X Edge. Type and confirm the status and configuration passphrase for the Edge.

Note

If you do not type the same passphrase when you add the device to VPN Manager, you cannot connect to the Firebox X Edge.

7 Click the **Enable Managed VPN** check box to configure the Firebox X Edge as a client to the WatchGuard DVCP server.

8 In the **DVCP Server Address** text box, type the IP address of the DVCP server.

9 Type the **Client Name** to give to your Firebox X Edge.
This is the name used to identify the Edge in VPN Manager.

10 Type the **Shared Key**.
The shared key is used to encrypt the connection between the DVCP Server and the Firebox X Edge. This shared key must be the same on the Edge and the DVCP Server. Get the shared key from your VPN administrator.

11 Click **Submit**.

Updating the Firebox X Edge Software

One advantage of your LiveSecurity® service is continuous software updates. As new threats appear and WatchGuard® adds product enhancements, you receive alerts to let you know about new versions of your Firebox® X Edge e-Series software. To install any firmware on the Edge, you must have a current LiveSecurity subscription. For Firebox® X Edge updates, see the WatchGuard web site at:

https://www.watchguard.com/archive/softwarecenter.asp (select Firebox X Edge)

There are two different procedures to install firmware updates. The first method uses a larger download and applies the firmware update on the Firebox X Edge automatically when you start it on a Windows computer. The second method uses a smaller download and allows you to apply the firmware updates with the Firebox X Edge configuration pages. If you do not use Windows, you must use the second procedure.

Method 1: Installing software automatically

The first method installs the Firebox X Edge e-Series firmware update from a Windows computer. Download the Software Update Installer to use this method. To use the Software Update Installer:

1 Start the installer on a Windows computer that is on the trusted network of the Firebox X Edge.

2 When you see the prompt, type the Firebox X Edge e-Series trusted interface IP address.
The default address is 192.168.111.1.

3 Type the administrator name and password. Click **OK**.
The installer applies the firmware update to the Firebox X Edge e-Series. As part of the update process, the Firebox X Edge restarts one or two times—this is usual.

4 Click **Finish**.

Note

Because the Installer uses FTP to transfer files, make sure your Firebox X Edge is not configured to deny FTP traffic. For more information, see “Denying FTP access to the Firebox X Edge” on page 90.

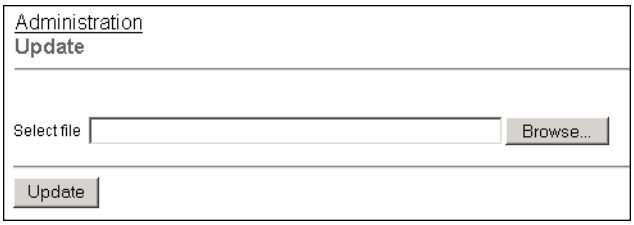
Method 2: Installing software manually

The second method uses the Firebox X Edge e-Series configuration pages. This method can be used with Windows or other operating systems. You must first download the Software Update file, which is a small compressed file.

1 Extract the "wgrd" file from the compressed file you downloaded with an archiving utility such as WinZip (for Windows computers), StuffIt (for Macintosh), or the zip program (for Linux).

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Administration** > **Update**.
The Update page appears.



3 Type the name and location of the file that contains the new Firebox X Edge software in the **Select file** box, or click **Browse** to find the file on the network.

4 Click **Update** and follow the instructions.
The Firebox makes sure the software package is a legitimate software upgrade. It then copies the new software to the system. This can take 15 to 45 seconds. When the update is complete, click the Reboot button that appears on the Update page. After the Firebox restarts, the System Status page appears and shows the new version number.

Activating Upgrade Options

All Firebox® X Edge e-Series devices include the software for all upgrade options. These options are activated when you install a license key on the Firebox. To get a license key, purchase and activate an upgrade option at the LiveSecurity service Web site or from a WatchGuard®-authorized reseller. See "Registering and Activating LiveSecurity Service" on page 20 for more information.

After you have purchased an upgrade option, you are given a license key. You use the license key to get the feature key for the upgrade. Use these steps to activate your license key and get your feature key:

1 Go to the upgrade page of the WatchGuard web site:
http://www.watchguard.com/upgrade

2 Type your LiveSecurity service user name and password in the fields provided.

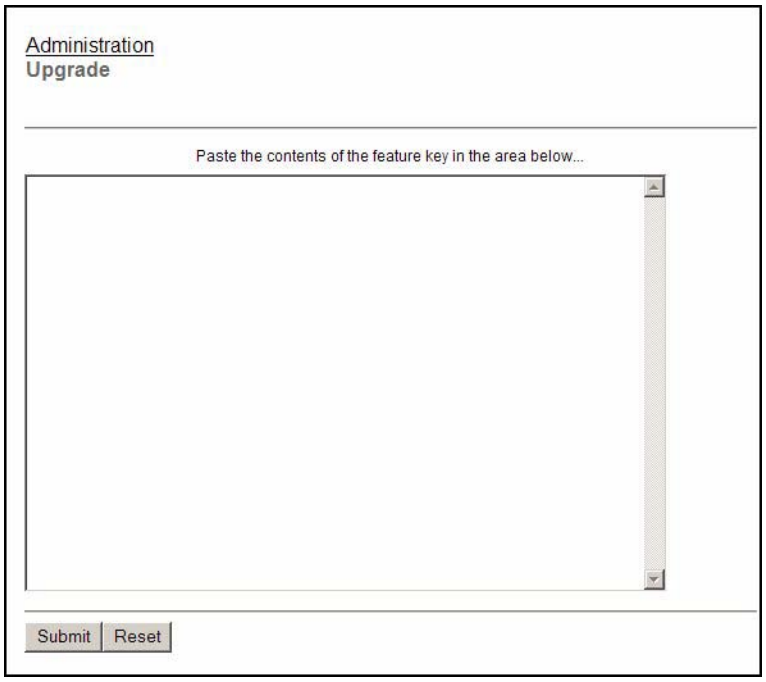
3 Click **Log In**.

4 Use the instructions on the web site to activate your license key and to get the feature key.

5 Copy the feature key from the LiveSecurity service web site.

6 To connect to the System Status page, type https:// in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

7 From the navigation bar, select **Administration** >**Upgrade**.
The Upgrade page appears.



8 Paste the feature key in the field.

9 Click **Submit**.

Upgrade options

User licenses

A seat license upgrade allows more connections between the trusted network and the external network. For example, a 5-seat user license upgrade allows five more connections to the external network.

MUVPN Clients

The MUVPN Clients upgrade allows remote users to connect to the Firebox X Edge through a secure (IPSec) VPN tunnel. These users have access to resources on the trusted and optional networks.

WebBlocker

The WebBlocker upgrade enables you to control access to Web content. For more information on WebBlocker, see Chapter 10, “Configuring WebBlocker.”

WAN Failover

The WAN failover feature adds redundant support for the external interface. For more information, see “Enabling the WAN Failover Option” on page 60.

Enabling the Model Upgrade Option

A model upgrade gives the Firebox® X Edge e-Series the same functions as a higher model. A model upgrade increases capacity, user licenses, sessions, and VPN tunnels. For a brochure that shows the features of the different Firebox X Edge models, go to:

http://www.watchguard.com/docs/datasheet/edge_ds.asp

You can upgrade a Firebox X Edge e-Series 10e or a Firebox X Edge 20e to a higher model:

1 Go to the upgrade site on the WatchGuard® web site (www.watchguard.com/upgrade) and log into your LiveSecurity service account.

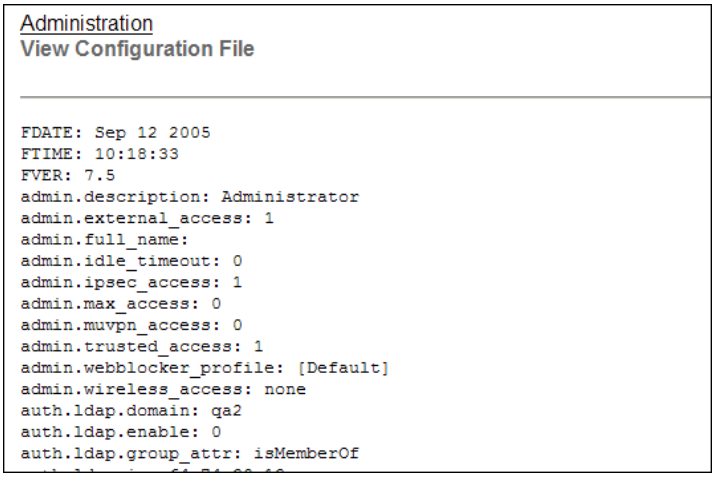
2 In the space provided, type the license key as it appears on your printed certificate or your online store receipt, including hyphens. Click **Continue** and follow the instructions.

Viewing the Configuration File

You can see the contents of the Firebox® X Edge configuration file in text format from the View Configuration page.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Administration** >**View Configuration File**.
The configuration file is shown.



CHAPTER 5

Changing Your Network Settings

A primary component of the WatchGuard® Firebox® X Edge e-Series setup is the configuration of network interface IP addresses. At a minimum, you must configure the external network and the trusted network to let traffic flow through the Edge. You do this when you use the Quick Setup Wizard after you install the Edge. You can use the procedures in this chapter to change this configuration after you run the Quick Setup Wizard.

You also can set up the optional interface. Many customers use the optional network for public servers. An example of a public server is a Web server.

Using the Network Setup Wizard

The easiest method to change the network IP addresses of the Firebox® X Edge e-Series is with the Network Setup Wizard.

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Wizards**.

3 Adjacent to **Setup the primary network interfaces of the Firebox X Edge**, click **Go**.

4 Follow the instructions on the screens.

The Network Setup Wizard has these steps:

Welcome
The first screen describes the purpose of the wizard.

Configure the external interface of your Firebox
Select the procedure your ISP uses to set your IP address. For more information, see the subsequent section in this guide, "Configuring the External Network."

Configure the external interface for DHCP
If your ISP uses DHCP, type the DHCP information that your ISP gave you. For more information, see "If your ISP uses DHCP" on page 46.

Configure the external interface for PPPoE
If your ISP uses PPPoE, type the PPPoE information that your ISP gave you. For more information, see "If your ISP uses PPPoE" on page 48.

Configure the external interface with a static IP address

If your ISP uses static IP addresses, type the static IP address information your ISP gave you. For more information, see "If your ISP uses static IP addresses" on page 47.

Configure the trusted interface of the Firebox

On this screen, type the IP address of the trusted interface. For more information, see "Configuring the Trusted Network" on page 50.

After you configure the trusted interface, the Network Setup Wizard is complete.

Configuring the External Network

You must configure your external network manually if you do not use the Network Setup Wizard.

When you configure the external network, set the method your ISP uses to give you an IP address for your Firebox® X Edge. There are three methods ISPs use to assign IP addresses:

- **DHCP** - Network administrators use DHCP to give IP addresses to computers on their network automatically. With DHCP, your Firebox receives an external IP address each time it connects to the ISP network. It can be the same IP address each time, or it can be a different IP address.
- **Static IP address** - Network administrators use static IP addresses to manually give an IP address to each computer on their network. A static IP address can be more expensive than a dynamic IP address because static IP addresses make it easy to set up servers. Static IP addresses are known also as manual addresses.
- **PPPoE** - Many ISPs use PPPoE (Point to Point Protocol over Ethernet) to give IP addresses to each computer on their network.

To configure your Edge, you must know how it gets the IP address for the external interface. If you do not know the method, get the information from your ISP or corporate network administrator.

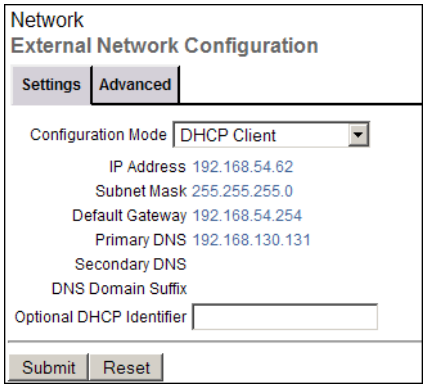
If your ISP uses DHCP

In the default configuration, the Firebox X Edge e-Series gets its external address information through DHCP. If your ISP uses DHCP, your Edge gets a new external IP address when it starts and connects to the ISP network. For more information about DHCP, see "About DHCP" on page 4.

To manually set your Firebox to use DHCP on the external interface:

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > External**.
The External Network Configuration page appears.



3 From the Configuration Mode drop-down list, select **DHCP Client**.

4 If your ISP makes you identify your computer to give you an IP address, type this name in the **Optional DHCP Identifier** field.

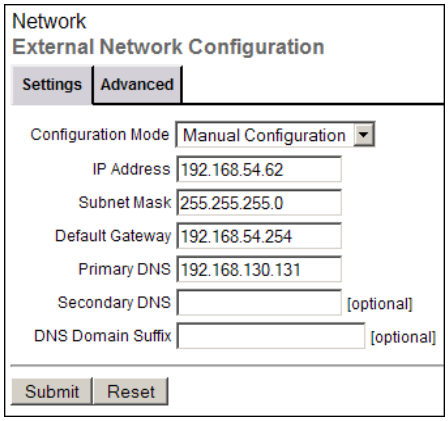
5 Click **Submit**.

If your ISP uses static IP addresses

If your ISP uses static IP addresses, you must enter the address information into your Firebox X Edge before it can send traffic through the external interface.

To set your Firebox X Edge to use a static IP address for the external interface:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > External**.
The External Network Configuration page appears.



2 From the **Configuration Mode** drop-down list, select **Manual Configuration**.

3 Type the IP address, subnet mask, default gateway, primary DNS, secondary DNS, and DNS domain suffix into the related fields. Get this information from your ISP or corporate network administrator.
If you completed the table on page 11, type the information from the table.

4 Click **Submit**.

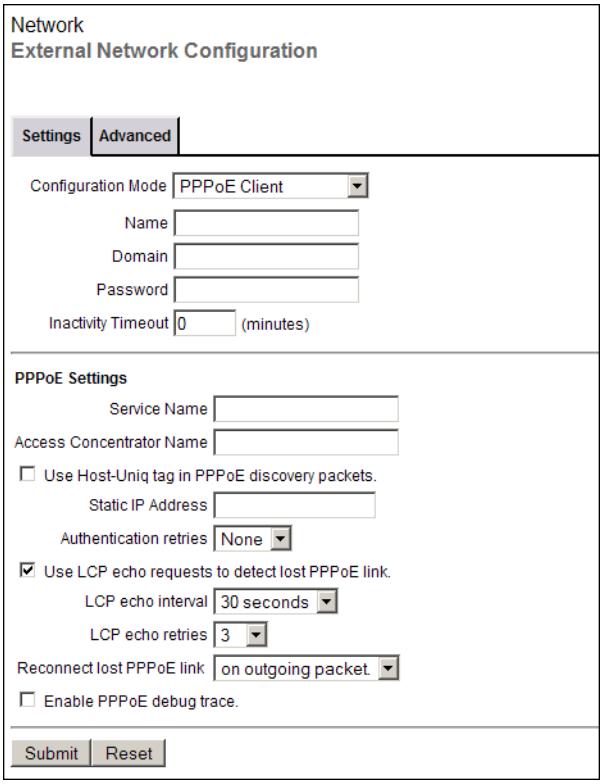
If your ISP uses PPPoE

If your ISP uses PPPoE, you must enter the PPPoE information into your Firebox X Edge before it can send traffic through the external interface. For more information in PPPoE, see "About PPPoE" on page 4.

To set your Firebox to use PPPoE on the external interface:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > External**.

The External Network Configuration page appears..



2 From the Configuration Mode drop-down list, select **PPPoE Client**

3 Type your name and password in the related fields. Get this information from your ISP. If your ISP gives you a domain name, type it into the **Domain** field.

Most ISPs using PPPoE make you use the domain name and your user name. Do not include the domain name with your user name like this: *myname@ispdomain.net*. If you have a PPPoE name with this format, type the myname section in the Name field. Type the ispdomain section in the Domain field. Do not type the @ symbol. Some ISPs do not use the domain.

4 In the **Inactivity Time-out** field, type the number of minutes before the Firebox X Edge disconnects inactive connections.

We recommend a value of 20.

5 Select **Automatic** from the **Link Speed** drop-down list to have the Edge select the best network speed, or select a static link speed that you know is compatible with your equipment.

We recommend that you set the link speed to Automatic unless you know this setting is incompatible with your equipment.

Advanced PPPoE Settings

The Quick Setup Wizard allows you to set up basic PPPoE settings. If necessary, you can also configure more advanced settings:

Service Name

Use this field to add a service name. The Firebox X Edge only starts with access concentrators that support the specified service. Usualy, this option is not used. Use this field only if there is more than one access concentrator or you know that you must use a specified service name.

Access Concentrator Name

Use this field to identify a PPPoE server, known as an access concentrator. The Firebox X Edge starts a session only with the access concentrator you identify in this field. Usually, this option is not used. Use it only if you know there is more than one access concentrator. If you enter a Service Name and Access Concentrator Name, you must use the same value for the Edge to negotiate a PPPoE session.

Use Host-Uniq tag in PPPoE discovery packets

Select this option if there is more than one installation of the same PPPoE client on the network. This can prevent interference between the discovery packets of each client. This is not a supported Firebox X Edge feature; this option is included to make the Edge compatible with ISPs which have this requirement.

Authentication retries

This field controls the number of times the Firebox X Edge tries to send PAP authentication information to the PPPoE server. The default value of None is sufficient for most installations. You must enter a high value to make the Edge compatible with some ISPs.

Use LCP echo request to detect lost PPPoE link

When you enable this check box, the Firebox X Edge sends an LCP echo request at regular intervals to the ISP to make sure that the PPPoE connection is active. If you do not use this option, the Edge must get a PPPoE or PPP session termination request from the ISP to identify a broken connection.

LCP echo interval

When you enable LCP echoes, this value sets the interval between LCP echo requests sent by the Firebox X Edge to the ISP. The more frequently the LCP echo requests are sent, the faster the Edge can identify a broken link. A shorter interval uses more bandwidth on the external interface, but even the shortest interval does not significantly decrease performance.

LCP echo retries

When you enable LCP echoes, this value sets the number of times the Firebox X Edge tries to get a response to an LCP echo request before the PPPoE connection is considered inactive. If an ISP does not send a reply to three LCP requests, there is a low probability that it will reply to subsequent LCP echo requests. In most cases, the default setting of three is the best.

Reconnect lost PPPoE link

This setting controls how and when the Firebox X Edge tries to restart a PPPoE connection after it is broken. The default value is **on outgoing packet**. With this option, the Edge tries to connect when a computer on the trusted or optional networks sends traffic to the external network. If you set the Edge to connect **immediately**, the Edge tries to connect when it finds that the PPPoE connection is broken.

Enable PPPoE debug trace

WatchGuard® Technical Support uses this check box to troubleshoot PPPoE problems. With this option on, the Firebox X Edge makes a file that you can send to Technical Support. Use this option only when Technical Support tells you because it decreases Edge performance.

Click **Submit** when you have completed the configuration of the Advanced PPPoE settings.

Configuring the Trusted Network

You must configure your trusted network manually if you do not use the Network Setup Wizard.

You can use static IP addresses or DHCP for the computers on your trusted network. The Firebox® X Edge e-Series has a built-in DHCP server to give IP addresses to computers on your trusted and optional networks. You can also change the IP address of the trusted network.

The factory default settings of a Firebox X Edge DHCP server automatically give IP addresses to computers on the trusted network. The trusted network starts with IP address 192.168.111.1. It is a "class C" network with a subnet mask of 255.255.255.0. The Edge can give an IP address from 192.168.111.2 to 192.168.111.254. The factory default settings use the same DNS server information on the internal and external interfaces.

If necessary, you can disable the DHCP server. Or, you can use the Edge as a DHCP relay agent and send DHCP requests to a DHCP server on a different network using a VPN tunnel. You can also use static IP addresses for the computers on your trusted network.

Any changes to the trusted network configuration page require that you click **Submit** and restart the Firebox X Edge before the new configuration is used. You can make many changes at one time and then restart just one time when you are done.

Changing the IP address of the trusted network

If necessary, you can change the trusted network IP address. For example, if you connect two or more Firebox X Edge devices in a virtual private network, each Edge must use a different trusted network address. If the two sides of the VPN use the same trusted network IP addresses, one side must change the trusted network IP address range so that it is different from the other side. For more information, see "What You Need to Create a VPN" on page 135.

Note

If you change the IP address of the Firebox X Edge trusted interface, you must use the new IP address in your browser address bar to connect to the Edge's web management interface. For example, if you change the Firebox X Edge trusted interface IP address from the default 192.168.111.1 to 10.0.0.1, then you must use https://10.0.0.1 to connect to the Firebox X Edge. Your computer's IP address must also be changed so that it is in the new trusted network IP subnet range.

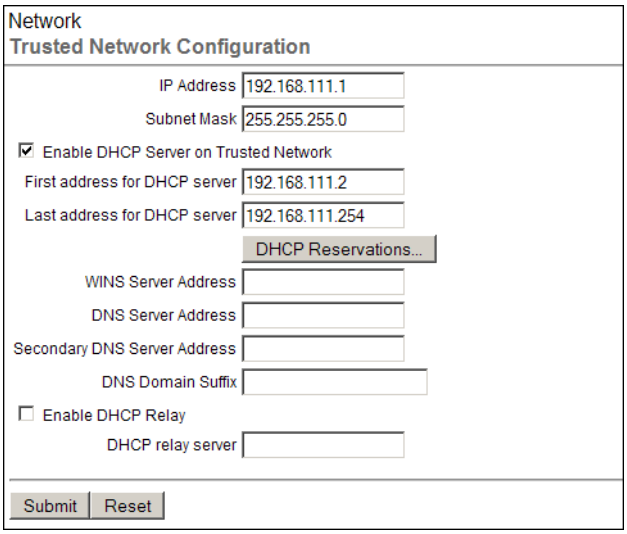
To change the IP address of the trusted network:

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.

3 Type the new IP address of the Firebox X Edge's trusted interface in the **IP Address** text field.

4 If necessary, type the new subnet mask.



Using DHCP on the trusted network

The DHCP Server option sets the Firebox X Edge e-Series to give IP addresses to the computers on the trusted network. When the Edge receives a DHCP request from a computer on the trusted network, it gives the computer an IP address. By default, the Edge has the DHCP Server option for the trusted interface enabled.

To use DHCP on the trusted network:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.

2 Select the **Enable DHCP Server on the Trusted Network** check box.

3 Type the first and last available IP addresses for the trusted network. Do not include the IP address of the Firebox X Edge.
The IP addresses must be on the same network as the trusted IP address. For example, if your trusted IP address is 192.168.200.1, the IP addresses can be from 192.168.200.2 to 192.168.200.254.

4 If you have a WINS or DNS server, type the **WINS Server Address**, **DNS Server Primary Address**, **DNS Server Secondary Address**, and **DNS Domain Suffix** in the correct text boxes.
If you do not enter a value, the Firebox X Edge uses the same values as those used for the external network.

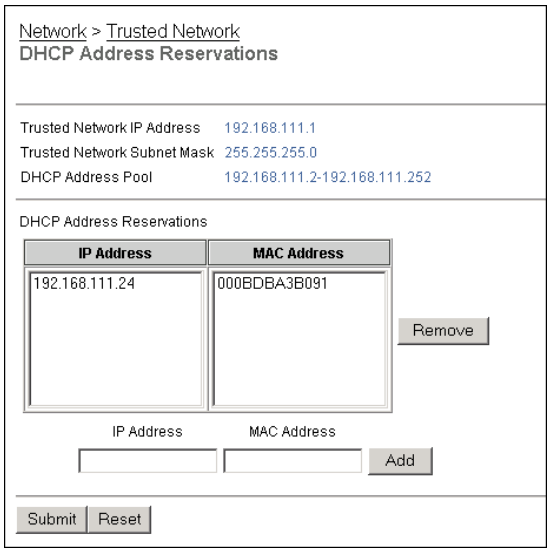
5 Click **Submit.**

Setting trusted network DHCP address reservations

You can manually give the same IP address to a specified computer on your trusted network each time that computer makes a request for a DHCP IP address. The Firebox X Edge identifies the computer by its MAC address.

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.

2 Click the **DHCP Reservations** button.
The DHCP Address Reservations page appears.



3 Type a static IP address in the **IP Address** field. The IP address must be on the trusted network.
For example, if the trusted network starts with 192.168.111.1, you can enter any address from 192.168.111.2 to 192.168.111.254.

4 Type the MAC address of the computer on the trusted network in the **MAC Address** field. You must enter the MAC address as 12 hexadecimal digits with no space, dash, or semicolon characters. Click **Add**.

5 Click **Submit**.

Configuring the trusted network for DHCP relay

One method to get IP addresses for the computers on the trusted network is to use a DHCP server on a different network. The Firebox X Edge e-Series can send a DHCP request to a DHCP server at a different location through a VPN tunnel. It gives the reply to the computers on the Edge trusted network. This option lets computers in more than one office use the same network address range. In this procedure the Edge is a DHCP Relay Agent. You must set up a VPN between the Edge and the DHCP server for this feature to operate correctly.

To configure the Firebox X Edge as a DHCP Relay Agent for the trusted interface:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.

2 Select the **Enable DHCP Relay** check box.

3 Type the IP address of the DHCP server in the related field.

4 Click **Submit.** You must restart the Firebox X Edge for new configuration to start.

Note

If the Firebox X Edge cannot connect to the DHCP server in 30 seconds, it uses its own DHCP server to give IP addresses to computers on the trusted network. You must enable the DHCP Server on the trusted network for the DHCP relay function to operate.

Using static IP addresses for trusted computers

You can use static IP addresses for some or all of the computers on your trusted network. If you disable the Firebox X Edge DHCP server and you do not have a DHCP server on your network, you must manually configure the IP address and subnet mask of each computer. For example, this is necessary when a client-server software application must use a static IP address for the server. Static IP addresses must be on the same network as the Edge trusted interface. Computers on the trusted network with static IP addresses must use the Edge trusted interface IP address for the default gateway.

To disable the Firebox X Edge DHCP server, clear the **Enable DHCP Server on the Trusted Network** check box on the Trusted Network Configuration page and click **Submit**.

Note

Computers on the trusted network must use the Firebox X Edge trusted interface IP address as the default gateway. If a computer does not use the Edge as the default gateway, it usually cannot get to the external network or the Internet.

Adding computers to the trusted network

You can connect as many as three computers to the trusted interface of the Firebox X Edge e-Series if you connect each computer to one of the Edge's Ethernet ports 0 through 2. You can use 10/100 BaseT Ethernet hubs or switches with RJ-45 connectors to connect more than three computers. It is not necessary for the computers on the trusted network to use the same operating system.

To add more than three computers to the trusted network:

1 Make sure that each computer has a functional Ethernet card.

2 Connect each computer to the network. For more information, see "Connecting the Edge to more than four devices" on page 15.

Configuring the Optional Network

The optional network is an isolated network for less secure public resources. By default, a Firebox® X Edge does not allow traffic from the optional network to get to the trusted network. The factory default settings do allow traffic that starts from the trusted network to get to the optional network, but you can restrict that traffic. For more information, see "Services for the Optional Network" on page 86.

Because traffic that is started from the optional network is usually not allowed to the trusted network, you can use the optional network for servers that other computers can connect to from the Internet, such as a web, e-mail, or FTP server. We recommend you isolate your private network from these servers because the public can connect to them. If a server on the optional network is attacked from the Internet, the attacker cannot get to the computers on the trusted network. The trusted network is the most secure location for your private network.

If your computer is on the optional network, you can connect to the Firebox X Edge system configuration pages using the optional interface IP address. The default URL for the System Status page from the optional network is: https://192.168.112.1

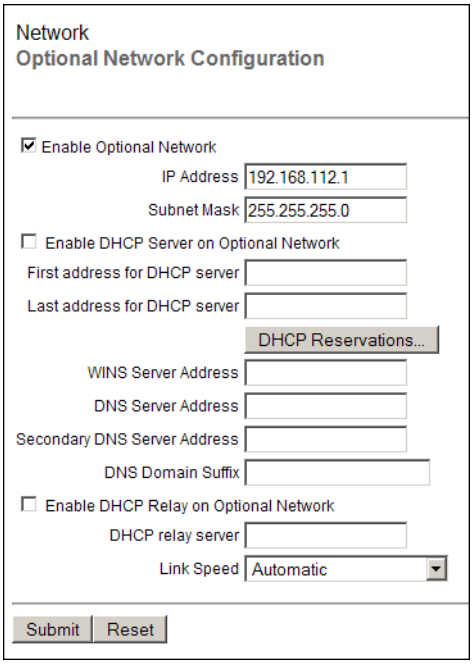
You can use the Firebox X Edge DHCP server or you can use static IP addresses for computers on the optional network. You also can change the IP address range of the optional network.

Enabling the optional network

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.

3 Select the **Enable Optional Network** check box.



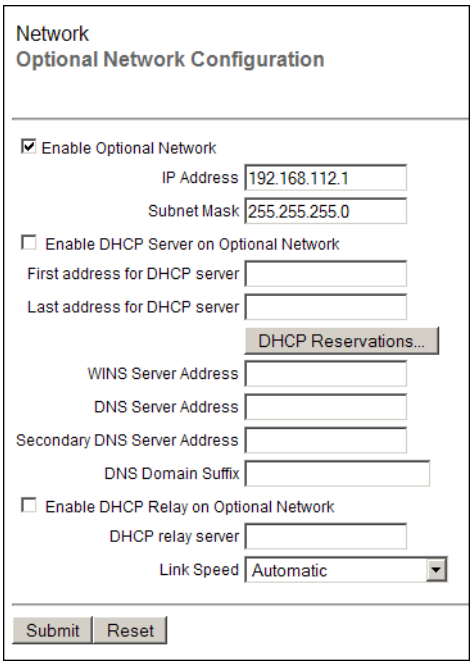
Changing the IP address of the optional network

If necessary, you can change the optional network address. By default, the optional interface IP address is set to 192.168.112.1, so the trusted network and the optional networks are on two different subnets. The IP address of the optional network cannot be on the same subnet as the trusted network.

To change the IP address of the optional network:

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.



3 In the **IP Address** text box, type the IP address to give the optional interface.

4 If necessary, type the new subnet mask.

5 Click **Submit**.

Using DHCP on the optional network

The DHCP Server option sets the Firebox X Edge to give IP addresses to the computers on the optional network. When the Edge receives a DHCP request from a computer on the optional network, it gives the computer an IP address. By default, the Edge has the DHCP Server option for the optional interface turned off.

To use DHCP on the optional network:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.

2 Select the **Enable DHCP Server on the Optional Network** check box.

3 Type the first available IP address for the optional network. Type the last available IP address.
The IP addresses must be on the same network as the optional IP address. For example, if your optional IP address is 192.168.112.1, the IP addresses can be from 192.168.112.2 to 192.168.112.254.

4 If you have a WINS or DNS server, type the **WINS Server Address**, **DNS Server Primary Address**, **DNS Server Secondary Address**, and **DNS Domain Suffix** in the related fields.
If you do not enter a value, the Firebox X Edge uses the same values as those used for the external network.

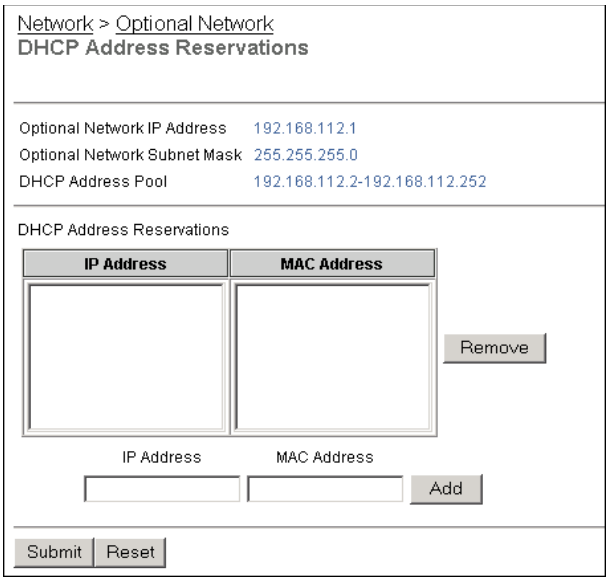
5 Click **Submit.**

Setting optional network DHCP address reservations

You can manually assign an IP address to a specified computer on your optional network. The Firebox X Edge identifies the computer by its MAC address.

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.

2 Click the **DHCP Reservations** button.
The DHCP Address Reservations page appears.



3 Type a static IP address in the **IP Address** field. The IP address must be on the optional network.
For example, if the optional network starts with 192.168.112.1, you can enter 192.168.112.2 to 192.168.112.251.

4 Type the MAC address of the computer on the optional network in the **MAC Address** field. You must enter the MAC address as 12 hexadecimal digits with no space, dash, or semicolon characters. Click **Add**.

5 Click **Submit**.

Configuring the optional network for DHCP relay

One method to get IP addresses for the computers on the Firebox X Edge optional network is to use a DHCP server on a different network. The Edge can send a DHCP request to a DHCP server at a different location and transmit the reply to the computers on the optional network. This option lets computers in more than one office use the same network address range. In this procedure, the Edge is a DHCP Relay Agent.

To configure the Firebox X Edge as a DHCP Relay Agent for the optional interface:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.

2 Select the **Enable DHCP Relay on Optional Network** check box.

3 Type the IP address of the DHCP server in the related field.

4 Click **Submit.** You must restart the Firebox X Edge for the new configuration to activate.

Note

If the Firebox X Edge cannot connect to the DHCP server in 30 seconds, it uses its DHCP server to give IP addresses to computers on the optional network. You must enable the DHCP server on the optional network for the DHCP relay function to operate.

Using static IP addresses for optional computers

You can use static IP addresses for some or all of the computers on your optional network. If you disable the DHCP server and you do not have a DHCP server on your optional network, you must manually configure the IP address and subnet mask of each computer. You also can configure specified devices with a static IP address. For example, this is necessary for a web server or network printer. Static IP addresses must be on the same network as the Firebox X Edge optional interface. Computers with static IP addresses on the optional network must use the optional interface IP address of the Edge as the default gateway or router.

To disable the Firebox X Edge DHCP server, clear the **Enable DHCP Server on the Optional Network** check box on the Optional Network Configuration page and click **Submit**.

Note

Computers on the optional network must use the Firebox X Edge optional interface IP address as the default gateway. If a computer does not use the Edge for the default gateway, it usually cannot get to the external network or the Internet.

Adding computers to the optional network

You can directly connect only one computer to the Firebox X Edge e-Series optional interface because there is only one optional Ethernet port. To connect more than one computer to the optional interface, use a 10/100 BaseT Ethernet hub or switch with RJ-45 connectors. It is not necessary for computers on the optional network to use the same operating system.

To add more than one computer to the optional network:

1 Make sure that each computer has a functional Ethernet card.

2 Set each computer to use DHCP. For more information, see "Setting Your Computer to Connect to the Edge" on page 17.

3 Connect each computer to the network. For more information, see "Connecting the Edge to more than four devices" on page 15.

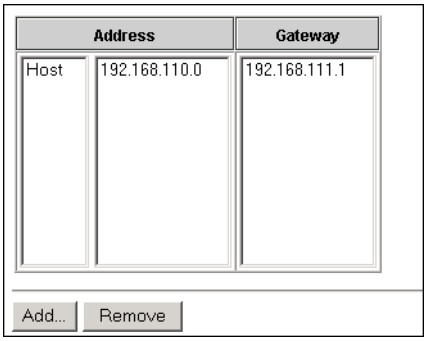
4 Restart each computer.

Making Static Routes

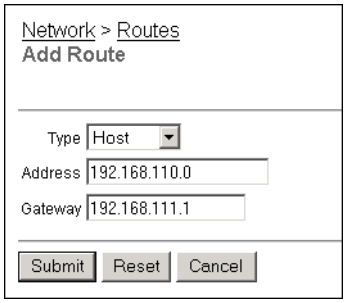
You can configure the Firebox® X Edge e-Series to send traffic to networks that are behind routers when you add static routes to these networks. Use the Routes page to make a static route:

1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Routes**.
The Routes page appears.



3 Click **Add**.
The Add Route page appears.



4 From the **Type** drop-down list, select **Host** or **Network.**
This box tells if the destination for the static route is one computer or a network of computers.

Note

A host is one computer. A network is more than one computer using a range of IP addresses.
You must type network addresses in "slash" notation (also known as CIDR, or Classless Inter Domain Routing, notation). Do not type a slash for a host IP address. For more information on how to enter IP addresses in slash notation, refer to this FAQ:
http://watchguard.com/support/advancedfaqs/general_slash.asp.
You must log in to your LiveSecurity account to see this FAQ.

5 Type the destination IP address and the gateway in the related fields.
The gateway is the local interface IP address of the router. The gateway IP address must be in the Firebox X Edge trusted, optional, or external network range.

6 Click **Submit**.

To remove a static route, click the IP address and click **Remove.**

Registering with the Dynamic DNS Service

You can register the external IP address of the Firebox® X Edge e-Series with the dynamic Domain Name Server (DNS) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to

your domain name changes when your ISP gives your Edge a new IP address. For more information, refer to these FAQs. You must log into your LiveSecurity Service account to see these FAQs:

What is Dynamic DNS?

http://watchguard.com/support/AdvancedFaqs/sogen_main.asp

How do I set up Dynamic DNS?

http://watchguard.com/support/AdvancedFaqs/sogen_setupdyndns.asp

Note

WatchGuard is not affiliated with DynDNS.org.

Create a DynDNS.org account

To set up your account, go to this web site:

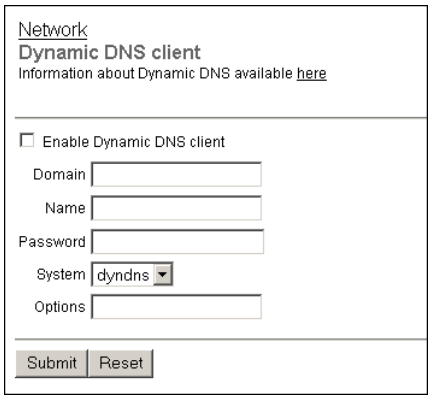
http://www.dyndns.org

This site also has information about how Dynamic DNS operates.

Set up the Firebox X Edge for Dynamic DNS

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Dynamic DNS**.
The Dynamic DNS client page appears.



3 Select the **Enable Dynamic DNS client** check box.

4 Type the **Domain**, **Name**, and **Password** in the related fields.

5 In the **System** drop-down list, select the system to use for this update.
The option dyndns sends updates for a Dynamic DNS host name. The option statdns sends updates for a Static DNS host name. The option custom sends updates for a Custom DNS host name. For an explanation of each option, see: http://www.dyndns.org/services/

6 In the **Options** field, you can type these options:

mx=mailexchanger
backmx=YES|NO

wildcard=ON|OFF|NOCHG
offline=YES|NO

See this site for more information:
http://www.dyndns.org/developers/specs/syntax.html

7 Click **Submit**.

Note

The Firebox X Edge gets the IP address of members.dyndns.org when it starts up. The Edge connects to the IP address it finds for members.dyndns.org to register the current Edge external interface IP address with the DynDNS service.

The Firebox X Edge does not operate with other Dynamic DNS services, only DynDNS.org.

Enabling the WAN Failover Option

The WAN Failover option supplies redundant support for the external interface. With this option, the Firebox® X Edge e-Series starts a connection through the WAN2 port when the primary external interface (WAN1) cannot send traffic. Companies use this option if they must have a constant Internet connection. You must have a second Internet connection to use this option. You can have a second broadband connection connected to the Edge to supply a failover Internet connection.

It is not necessary to configure new services to use this option. The failover interface uses the same services and network properties as the external interface.

The Firebox X Edge e-Series uses two procedures to see if the external interface is functional:

- The status of the link between the external interface and the device it is connected to (usually a router)
- A ping command to a specified location

The Firebox X Edge sends a ping to the default gateway or a computer specified by the administrator. If there is no reply, the Edge changes to the secondary external network interface (WAN2).

When you enable the WAN Failover feature, the Firebox X Edge e-Series does this:

- If the WAN1 interface connection stops, the Edge starts to use the WAN2 interface.
- If the WAN2 interface connection stops, the Edge starts to use the WAN1 interface.
- If the WAN1 interface and the WAN2 interface stop, the Edge tries the two interfaces until it makes a connection.

When the WAN2 interface is in use, the Firebox X Edge monitors the primary (WAN1) interface. When the WAN1 interface becomes available, the Edge automatically goes back to using the WAN1 interface.

To configure the WAN failover network:

1 Connect one end of a straight-through Ethernet cable to the WAN2 interface. Connect the other end to the source of the secondary external network connection. This connection can be a cable modem or a hub.

2 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

3 Configure the failover network with the WAN Failover Setup Wizard or with the Network page of the configuration pages, as described in the subsequent two sections.

Using the WAN Failover Setup Wizard

1 From the navigation bar, select **Wizards**.

2 Adjacent to **Configure the automatic WAN failover capability of your Firebox Edge**, click **Go**.

3 Use the instructions on the screens.

The WAN Failover Setup Wizard includes these steps:

Welcome

The first screen tells you about the wizard.

Select the secondary interface

Use this screen to set the secondary interface your Firebox X Edge uses.

Configure the broadband interface

If you use a broadband interface, select the method your ISP uses to get your IP address.

Identify the computers to connect

Type the IP addresses of computers to which the Firebox X Edge can connect.

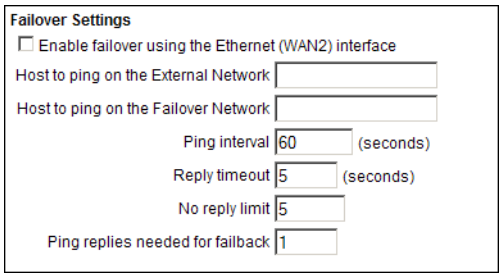
The WAN Failover Setup Wizard is complete

You must restart your Firebox X Edge to activate the WAN Failover feature.

Using the Network page

1 From the navigation bar, select **Network > WAN Failover**.

The WAN Failover page appears.



2 Select the **Enable failover using the Ethernet (WAN2) interface** check box.

3 Type the IP addresses of the hosts to ping for the WAN1 (external) and WAN2 (failover) interfaces.

The Firebox X Edge will send pings to the IP addresses you type here. If pings to the host on that network are not successful, the Edge starts the failover. You control the frequency of pings in the fields below.

4 Type the number of seconds between pings and the number of seconds to wait for a reply.

5 Type the maximum number of pings before time-out in the **No Reply Limit** field.

6 Type the number of successful pings that must be made before the Firebox X Edge uses the WAN1 interface again in the **Ping replies needed for failback** field.

If you are using a broadband connection for failover

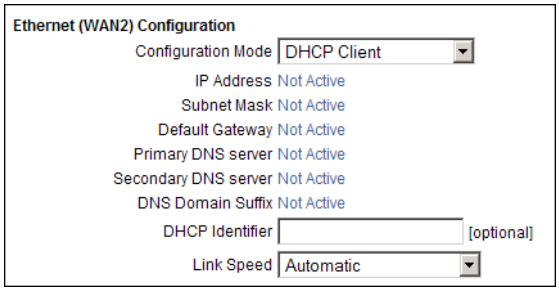
If you selected to enable failover with an Ethernet connection on WAN2, select your configuration mode from the drop-down list:

1 If your IP address is assigned automatically, select **DHCP Client**.

2 If you have a static IP address, select **Manual Configuration**.

3 If your IP address is assigned using PPPoE, select **PPPoE Client**.

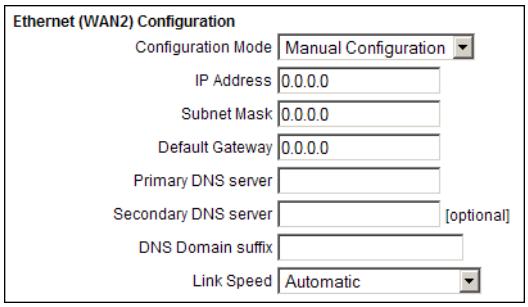
If you selected DHCP Client



1 If you must identify your computer when you request an IP address, type the name in the **Optional DHCP Identifier** field. If necessary, adjust the link speed from the drop-down list.

2 Click **Submit**.

If you selected Manual Configuration



1 Type the IP address, subnet mask, default gateway, primary DNS, secondary DNS, and DNS domain suffix. If necessary, select the appropriate link speed from the drop-down list.

If you completed the table on page 11, type the information from the table. If you do not have this information, speak with your ISP or corporate network administrator.

2 Click **Submit**.

If you selected PPPoE

See "If your ISP uses PPPoE" on page 48 for information on PPPoE settings. Configure the WAN2 interface using that information.

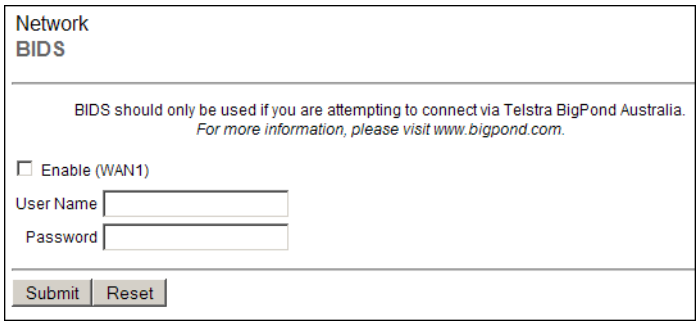
Configuring BIDS

Telstra customers in Australia must use client software to connect to the BigPond network. The Firebox® X Edge e-Series uses BIDS to make this connection. If you do not connect to the BigPond network, it is not necessary to use BIDS.

To configure your Firebox to connect to the BigPond network using BIDS:

1 To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > BIDS**.
The BIDS client page appears.



3 To enable BIDS, select the **Enable (WAN1)** check box.

4 Type your login information in the **User Name** and **Password** text boxes.

5 Click **Submit**.
The BIDS information is used to connect to the BigPond network.

CHAPTER 6

Firebox X Edge e-Series Wireless Setup

Wireless networks use RF (radio frequency) signals to send and receive traffic from computers. The Firebox® X Edge e-Series Wireless protects the computers that are connected to your network and it protects your network wireless connections. The Edge Wireless obeys the 802.11b and 802.11g guidelines set by the Institute of Electrical and Electronics Engineers (IEEE). This chapter examines how to install the Edge Wireless and set up the wireless network.

By default, the wireless features of your Firebox X Edge e-Series are disabled for more security. You must enable the wireless feature after you complete the Edge Wireless Quick Setup wizard.

To install the Firebox X Edge Wireless:

- Identify and record your TCP/IP settings
- Disable the HTTP proxy settings of your web browser
- Activate DHCP on your computer
- Make a physical Ethernet connection between the Firebox X Edge e-Series Wireless and your network. You must connect to the Edge with a wired connection to configure its wireless properties.
- Attach the two antennae to the Firebox X Edge e-Series Wireless.
- Install the Firebox X Edge e-Series Wireless in a location more than 20 centimeters from all persons. This is an FCC requirement for low power transmitters.
- Put the Firebox X Edge e-Series Wireless in a location away from other antennae or transmitters to decrease interference.

To set up the wireless network:

- Select and configure the Firebox X Edge trusted or optional networks
- Configure the Wireless Access Point (WAP)
- Configure the wireless adapter on your computer

Connecting to the Firebox X Edge e-Series Wireless

The Firebox® X Edge e-Series Wireless can protect one computer, or all the computers that connect to your network. The Edge Wireless uses switch functionality to connect other computers.

To set up a wireless network, connect a computer with a web browser to the Firebox X Edge e-Series Wireless with an Ethernet cable.

Use this computer to configure the wireless network.

See "Connecting the Edge to more than four devices" on page 15 for information about connecting computers, printers, or other devices that connect directly to the Firebox X Edge Wireless.

Using the Wireless Network Wizard

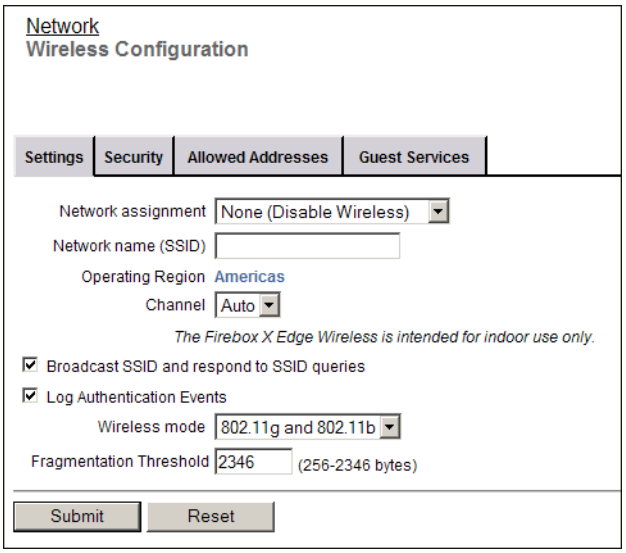
The Wireless Network Wizard is a tool that you use to automatically configure your Firebox® X Edge wireless network. To start the wizard, select **Wizards** from the navigation bar and click **Go** adjacent to the task: **Configure the wireless network interface of the Firebox X Edge**.

Configuring Basic Wireless Settings

If you do not use the Wireless Network Wizard, or if you want to change wireless settings manually, you can use the Firebox X Edge e-Series Wireless configuration page.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Wireless (802.11g)**.



The Wireless Configuration page appears, with the Settings tab active.

Note

When you complete the wireless configuration, restart your Firebox X Edge e-Series Wireless.

Selecting the wireless network assignment

The **Network Assignment** drop-down list gives you three alternatives to select from:

None (disable wireless)

In this mode, the wireless feature is disabled.

Bridge to Trusted

In this mode, the wireless client is a part of the trusted network. If the wireless client sets the IP address of its wireless network card with a static IP address, the IP address must be in the trusted IP address range of the Firebox X Edge. If the wireless network card is set to DHCP, the DHCP server on the Edge's trusted network must be active and configured. If this option is selected, the wireless client can send any type of traffic to the other computers on the trusted network. This includes Windows Networking NetBIOS broadcasts, which are useful for users who browse with Windows Network Neighborhood.

Bridge to Optional

In this mode, the wireless client is a component of the optional network. You must use the Bridge to Optional mode if you enable guest services on the Firebox X Edge e-Series Wireless. If you use this option, you must first activate the optional network. The optional network is not

enabled by default. If the wireless client has its wireless network card set with a static IP address, the IP address must be in the optional IP address range of the Edge. If the wireless network card is set to DHCP, the DHCP server on the Edge's optional network must be active and configured. If this option is selected, the wireless client can send any type of traffic to the other computers on the optional network. This includes Windows Networking NetBIOS broadcasts.

Because the wireless client is a part of the optional network or trusted network, it is important to think about the networking requirements of wireless clients. The firewall properties control the traffic between these two networks.

Note

Because they are optional or trusted network clients, a wireless client can be a part of any Branch Office VPN tunnels in which the local network component of the Phase 2 settings include optional or trusted network IP addresses. To control access to the VPN, you can force Firebox X Edge users to authenticate.

Setting the SSID

The SSID (Service Set Identifier) is the unique name of your wireless network. To use the wireless network from a client computer, the wireless network card in your computer must have the same SSID as the Firebox X Edge e-Series Wireless.

To change the SSID of the Firebox X Edge e-Series Wireless, type a new name in the **SSID** field to uniquely identify your wireless network.

Setting the operating region and channel

There are eight options for operating region: Americas, Asia, Australia, EMEA, France, Israel, Japan and the People's Republic of China. This parameter is configured when you use the Quick Setup Wizard and cannot be changed after it is set. Your Firebox X Edge e-Series can have this option set at manufacturing.

The set of channels available for each operating region are in the **Channel** drop-down list. With the channel set to **Auto**, the Firebox X Edge e-Series Wireless automatically selects the channel with the strongest signal available in its physical location.

Controlling SSID broadcasts

Computers with wireless network cards send requests to see if there are wireless access points to which they can connect. To configure the Firebox X Edge e-Series Wireless to send and answer these requests, select the **Broadcast SSID and respond to SSID queries** check box. For security, turn this option on only when you are configuring computers on your network to connect to the Edge. Disable this option after all your clients are configured. If you use the wireless guest services feature, it can be necessary to allow SSID broadcasts in standard operation.

Logging authentication events

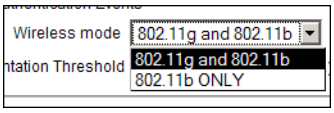
An authentication event occurs when a wireless computer tries to connect to the Firebox X Edge e-Series Wireless. To have the Edge record these events in the log file, select the **Log Authentication Events** check box. Use this option to add entries to the log when someone tries to access your wireless network.

Setting the wireless mode

Most wireless cards can operate only in 802.11b (up to 11 MB/second) or 802.11g (54 MB/second) mode. To set the operating mode for the Firebox X Edge e-Series Wireless, select an option from the **Wireless Mode** drop-down list. There are two wireless modes:

802.11g and 802.11b
This is the default mode. This mode allows the Edge to connect with devices that use 802.11b or 802.11g.

802.11b only
This mode allows the Edge to connect to devices using only 802.11b.



Note

The Firebox X Edge e-Series Wireless only operates in 802.11g mode if all the wireless cards connected to the Edge are using 802.11g. If any 802.11b clients connect to the Edge, all connections automatically drop to 802.11b mode.

Setting the fragmentation threshold

The Firebox X Edge e-Series Wireless allows you to set the maximum frame size it can send without fragmenting the frame. This is called the fragmentation threshold. This setting is rarely changed. It is set at the default maximum frame size of 2346, which means that it will never fragment any frames that it sends to wireless clients. This is best for most environments.

To change the fragmentation threshold, type a value in the **Fragmentation Threshold** field. The possible values are 256 through 2346. For more information on the fragmentation threshold parameter, see this FAQ:

www.watchguard.com/support/advancedfaqs/edge_fragthreshold.asp

You must log in to your LiveSecurity account to see this FAQ.

Configuring Wireless Security Settings

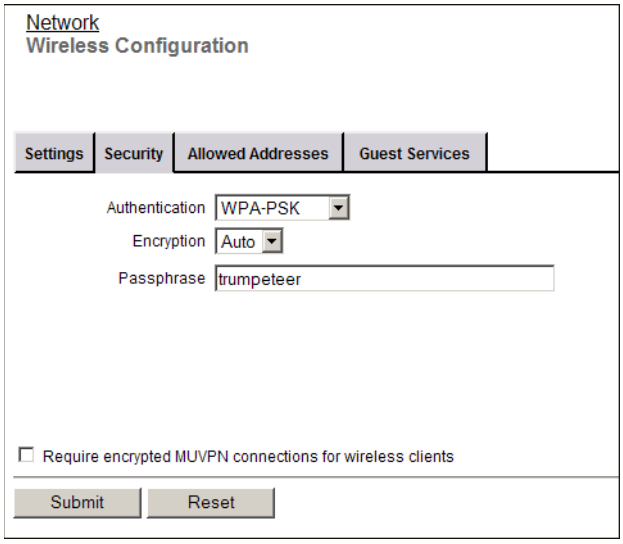
The Firebox® X Edge e-Series Wireless uses two security protocol standards to protect your wireless network. They are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WEP and WPA encrypt the transmissions on the wireless LAN between the computers and the access points. WPA and WEP also can prevent unauthorized access to the wireless access point.

WEP and WPA each use pre-shared keys, but WPA uses an algorithm to change the encryption key at regular intervals. This keeps the data sent on a wireless connection more secure. If you use the Windows XP operating system with Service Pack 2 or higher, you can use WPA-PSK (WPA with pre-shared keys) with no additional driver installation. If you use an earlier version of Windows or a different operating system, it can be necessary to install other drivers to use WPA-PSK. If you cannot use WPA-PSK, we recommend that you use Shared Key authentication with WEP encryption or MUVPN without WPA or WEP.

To protect privacy, you can use these features together with other LAN security mechanisms such as password protection, VPN tunnels, and user authentication.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Wireless (802.11g)** and click the **Security** tab.



Setting the wireless authentication method

Select the authentication method to use for your wireless network connection. The options are **Open System**, **Shared Key**, and **WPA-PSK**.

Open System

Open System authentication allows any user to authenticate with the access point. This method can be used with no encryption, or with WEP encryption. Although Open System authentication is the default authentication method for some versions of Microsoft Windows, other methods are more secure.

Shared Key

In Shared Key authentication, only those wireless clients that have the shared key can connect. This is more secure than Open System authentication. Shared Key authentication can be used only with WEP encryption.

WPA-PSK

PSK (pre-shared key) is the only WPA authentication method the Firebox X Edge e-Series Wireless supports at this time.

Configuring encryption

From the **Encryption** drop-down list, select the level of encryption for your wireless connections. The options change when you use different authentication mechanisms.

Open system and shared key authentication

Encryption options for open system and shared key authentication are WEP 64-bit hexadecimal, WEP 40-bit ASCII, WEP 128-bit hexadecimal, and WEP 128-bit ASCII. If you select open system authentication, you also can select no encryption.

1 If you use WEP encryption, type hexadecimal or ASCII characters in the **Key** text boxes. Not all wireless adapter drivers support ASCII characters.

You can have a maximum of four keys.
- A WEP 64-bit hexadecimal key must have 10 hexadecimal (0-f) characters.
- A WEP 40-bit ASCII key must have 5 characters.
- A WEP 128-bit hexadecimal key must have 26 hexadecimal (0-f) characters.
- A WEP 128-bit ASCII key must have 13 characters.

2 If you typed more than one key, click the key to use as the default key from the **Key Index** drop-down list.

The Firebox X Edge e-Series Wireless can use only one key at a time. If you select a key other than the first key in the list, you also must set your wireless client to use the same key.

WPA-PSK authentication

The encryption options for WPA-PSK authentication are TKIP, AES, and Auto. WPA-PSK operates correctly only if you are using Windows XP Service Pack 2 or higher or have installed a driver for your operating system that supports PSK.

We recommend that you set the WPA-PSK encryption option to **Auto** to have the Firebox X Edge e-Series Wireless accept TKIP and AES settings.

Configuring wireless clients to use MUVPN

To make wireless computers authenticate as MUVPN clients:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.

The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Network > Wireless** and click the **Security** tab.

3 Select the check box **Require encrypted MUVPN connections for wireless clients**.

If you use WEP/WPA encryption and use encrypted MUVPN at the same time, network speeds decrease.

4 Click **Submit**.

For more information, see "Configuring the MUVPN Client" on page 145.

Restricting Wireless Access by MAC Address

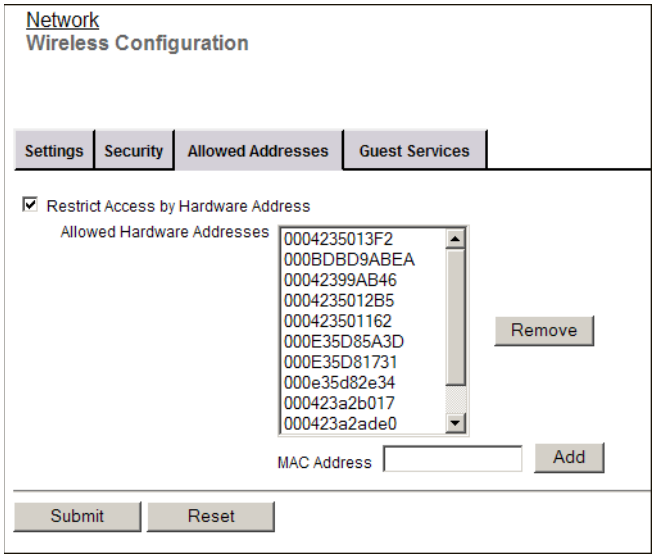
You can control access to the Firebox®X Edge e-Series Wireless by computer hardware (MAC) address. If this feature is enabled, and the MAC address of a computer that tries to connect to the Edge Wireless is not included in this configuration, the connection fails.

When you restrict wireless access by MAC address, it is possible that a hacker can get access to the wireless network by spoofing an allowed MAC address. Use authentication and encryption together with MAC address restrictions to keep your wireless network connections secure.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.

The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Wireless (802.11g)** and click the **Allowed Addresses** tab.



3 Select the **Restrict Access by Hardware Address** check box.

4 Type the MAC address of the computer that is allowed to connect to the Firebox X Edge Wireless in the correct field.
Look for the physical address of the wireless adapter.

5 Click **Add**.
Repeat steps 3–4 for each computer that can connect to the Edge.

6 Click **Submit**.

Configuring Wireless Guest Services

The Firebox® X Edge e-Series Wireless includes a default local user account called "guest." A guest is a wireless user that is not usually connected to the wireless network. A guest could be a business associate visiting your organization and given temporary access to the Internet, or possibly to your trusted network. You also can use guest services if you use your Edge to host wireless users other than the users the Edge is protecting with its firewall.

Note

Both guests and regular Firebox X Edge e-Series Wireless users can get access to the Edge through the wireless interface. Guest users can connect to all regular Edge user computers on the wireless network and Edge users can connect to all guest user computers. If you host wireless access for people outside your organization and keep other security settings low, the confidentiality of your data is at risk.

When guest services are enabled:

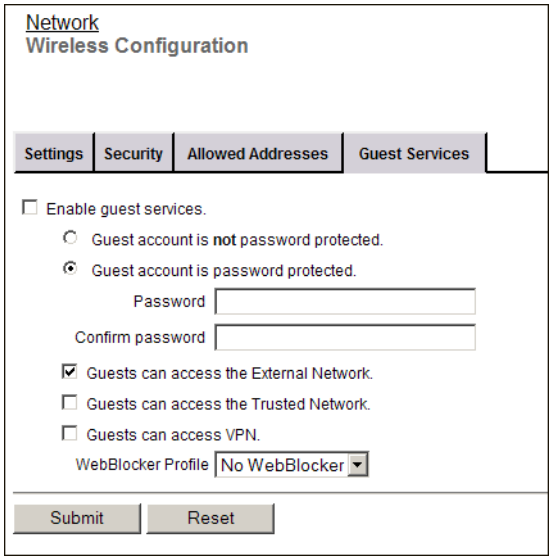
- The **Network Assignment** must be set to **Bridge to Optional Network** on the Wireless Configuration page.
- You must disable MAC address filters, or add the MAC address of each guest to the Allowed Hardware Addresses list.

- The guest user account is enabled. You can make users authenticate with a password, or without a password.

Enabling guest services

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Network > Wireless** (802.11g) and click the **Guest Services** tab.



3 Select the **Enable guest services** check box to turn on the guest service feature.
When you enable this feature, you also enable the default local user account "guest." Any user who gets access to the Firebox X Edge e-Series Wireless as a guest user must use the local user account named "guest." You cannot change the default name of the guest account.

Setting password protection

When a guest user connects to the wireless network using the Firebox X Edge e-Series Wireless as the wireless access point, you can make the user type a password, or you can disable password protection. If you disable password protection, the user does not have to type a password when they connect to the network.

Setting network access rules for guests

You can set the level of network access a guest user has on the Wireless Guest Services configuration page.

Guests can access the External Network

When this check box is selected, all wireless guests can use the Firebox X Edge e-Series Wireless as their access point to use resources on the external network. This option is selected by default so that all guest users have access to the Internet.

Guests can access the Trusted Network

Select this check box to allow guest users to use resources on the trusted or optional network protected by the Firebox X Edge e-Series Wireless.

Guests can access VPN

Select this check box to allow guest users to access VPN tunnels through the Firebox X Edge e-Series Wireless.

WebBlocker Profile

If you use WebBlocker, the options in this drop-down list control the types of web sites guest users can get access to through the Firebox X Edge e-Series Wireless. You can apply any existing WebBlocker profile to guest users. If this option is set to **No WebBlocker**, all guest users have full access to all web sites.

Connecting to the Edge as a wireless guest

To log on as a wireless guest user, a user must open their web browser and do one of these procedures:

- Type `https://` in their browser address bar, and the IP address of the Firebox X Edge trusted interface.
  The default URL is: https://192.168.111.1
- Try to get access to any HTTP web site on the Internet. The Edge automatically redirects the user to the login web page.
  The Edge does not automatically redirect a user who tries to get access to an HTTPS web site.

The user must type "guest" as the user name. If password protection is not required, the user does not have to type a password in the password text box. They can keep the text box blank and click **OK**.

Configuring the Wireless Card on Your Computer

These instructions are for the Windows XP with Service Pack 2 operating system. To see the installation instructions for other operating systems, go to:

http://www.watchguard.com/support/sohoresources/

To set up a wireless connection using Windows XP SP2:

1 Click **Start > Settings > Control Panel > Network Connections**.
The Network Connections dialog box appears.

2 Right-click **Wireless Network Connection** and select **Properties**.
The Wireless Network Connection dialog box appears.

3 Select the **Wireless Networks** tab.

4 Below **Preferred Networks**, click **Add**.
The Wireless Network Properties dialog box appears.

5 Type the SSID in the **Network Name (SSID)** text box.

6 Select the network authentication and data encryption methods from the drop-down lists.
If necessary, clear the check box labeled **The key is provided for me automatically** and type the network key two times.

7 Click **OK** to close the **Wireless Network Properties** dialog box.

8 Click the **View Wireless Networks** button.
All available wireless connections appear in the Available Networks text box.

9 Select the SSID of the wireless network and click **Connect**.
If the network uses encryption, type the network key twice in the Wireless Network Connection dialog box and click **Connect** again.

10 Configure the wireless computer to use DHCP. For more information about how to configure DHCP, see "Setting Your Computer to Connect to the Edge" on page 17.

The Firebox X Edge e-Series Wireless is configured to protect the wired and wireless computers that are attached to it from security risks.

CHAPTER 7

Configuring Firewall Settings

The Firebox® X Edge e-Series uses services and other firewall options to control the traffic between the trusted, optional, and external networks. The configuration of allowed services and firewall options sets the level of security the Edge applies to your network.

About This Chapter

The section "Configuring Outgoing Services" on page 83 shows you how to control traffic to the external network from the trusted and optional networks.

The section "Services for the Optional Network" on page 86 shows you how to control traffic between the trusted and optional networks. This section also has examples of how to use the optional network.

Other sections show how to use the Blocked Sites feature and other firewall options:

- Responding to pings
- Creating log messages for all outgoing traffic
- Setting FTP access to the Firebox® X Edge e-Series
- Changing the MAC address of the external interface

About Services

A Firebox® X Edge service is one or more rules that together monitor and control traffic. These rules set the firewall actions for a service:

- **Allow** lets data or a connection through the Edge.
- **Deny** stops data or a connection from going through the Edge, and sends a response to the source.
- **No Rule** sets a rule to off, as if the rule was not defined. This option is available to allow you to manage only the incoming or only the outgoing properties of a service.

For example, to operate a web server behind the Firebox X Edge e-Series, you must configure the HTTP service to allow traffic to the IP address of the web server.

Incoming and outgoing traffic

Traffic that comes from the external network is incoming traffic. Traffic that goes to the external network is outgoing traffic. By default, the Firebox X Edge e-Series denies incoming traffic to protect your trusted and optional networks.

The default configuration of the Edge allows this traffic:

- From the trusted network to the external network
- From the trusted network to the optional network
- From the optional network to the external network

The default configuration of the Edge denies this traffic:

- From the external network to the trusted network
- From the optional network to the trusted network
- From the external network to the optional network

Traffic through VPN tunnels

When you create a Mobile User VPN tunnel from remote users, or when you create a Branch Office VPN tunnel to other offices, the Firebox X Edge e-Series automatically allows all traffic through that VPN tunnel. No other configuration is necessary after the VPN tunnel is set up.

Configuring Incoming Services

You can control the traffic that goes to the trusted or optional networks from the external network using incoming services. Usually, the Internet is the external network.

The Firebox® X Edge supplies a list of frequently used services, called common services, that you can use to easily allow the most common traffic categories into your trusted or optional network. You also can create custom services if you must allow traffic that is not in the list of frequently used services.

You must be careful when you allow incoming services. When you allow an incoming service, you open the protected networks behind the Firebox X Edge to more traffic, which increases risk. Make sure that you compare the value of added access to the security risk.

Note

The incoming services in this section have no effect on traffic between the trusted and optional networks. These services also have no effect on traffic between computers on the trusted network or between computers on the optional network.

Configuring common services for incoming traffic

The Firebox X Edge e-Series includes standard services known as common services that you can use to control traffic through the Edge. You can use the procedure below to configure the properties of a common service.

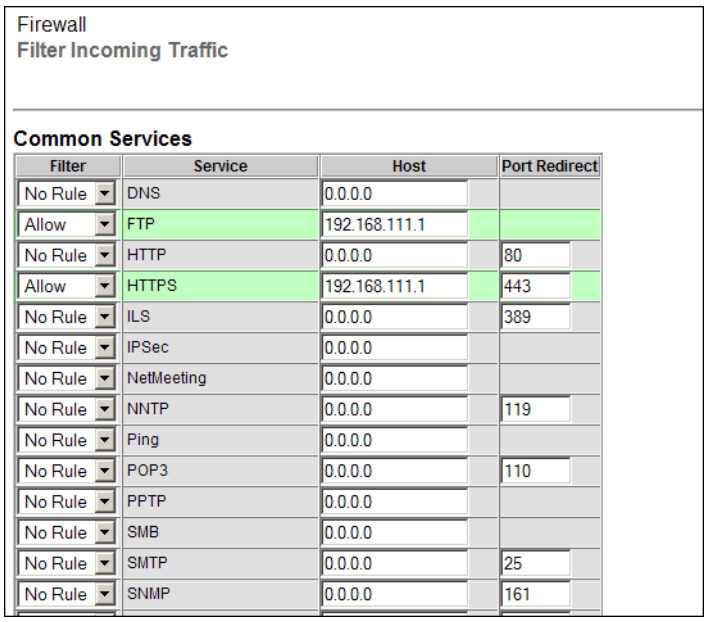
For more information on common services, refer to the list at the end of this FAQ:

www.watchguard.com/support/Tutorials/stepsoho_blockoutservice.asp

You must log in to your LiveSecurity account to see this FAQ.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Firewall** > **Incoming**.
The Filter Incoming Traffic page appears.



3 Find the common service to allow into your trusted or optional network from the external network. From the **Filter** drop-down list adjacent to the service name, select **Allow** or **Deny**.
If you select No Rule, the traffic is denied unless you create a custom service to allow that traffic.
For more information, see "Adding a custom incoming service manually" on page 80, or "Adding a custom service using the wizard" on page 85.

4 If you allow the service, enter the IP address of the service host.
The service host is the computer on the trusted or optional network that receives the traffic.

5 If you redirect the service to another port, type the port number.
For more information, see "Working with Firewall NAT" on page 97.

6 Click **Submit**.

7 Repeat steps 1-6 to allow or deny more common services.

Note

If you set a common service to Allow, the Firebox X Edge allows traffic that uses that service from any source on the external network. Traffic from that service goes to the service host.
To limit the external sources that can use the ports and protocols of the service you are adding, create a custom service.

About custom services for incoming traffic

A custom service for incoming traffic is necessary if:

- Incoming traffic does not use the same ports or protocols used by one of the common services.
- You restrict the IP addresses on the external network that can connect to a computer behind the Firebox X Edge e-Series.

You can add a custom service using one or more of these:

- TCP ports
- UDP ports
- An IP protocol that is not TCP or UDP. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

Adding a custom service using the wizard

1 From the navigation bar, click **Wizards**.

2 Adjacent to **Define a custom service**, click **Go**.

3 Use the instructions in the wizard to add a custom service.

The Traffic Filter Wizard includes these steps:

Welcome
The first screen tells you about the wizard and the information you must have to complete the wizard.

Service Name
Type a name to identify the service.

Protocols and Ports
Set the protocol and ports to assign to this traffic filter.

Traffic Direction
Identify if this is an incoming or outgoing service.

Service action
Configure the Edge to allow or deny this type of service traffic through the firewall.

Restrict to remote computers
To put a limit on the scope of the service, add the IP addresses of the computers or networks outside the firewall to which this service applies.

Restrict to local computers
To put a limit on the scope of the service, add the IP addresses of the computers or networks inside the firewall to which this service applies.

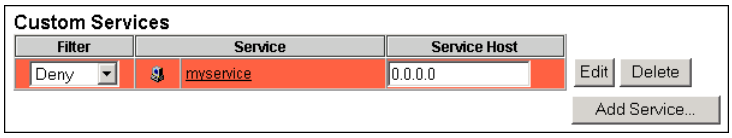
Adding a custom incoming service manually

You can add a custom service without using the wizard.

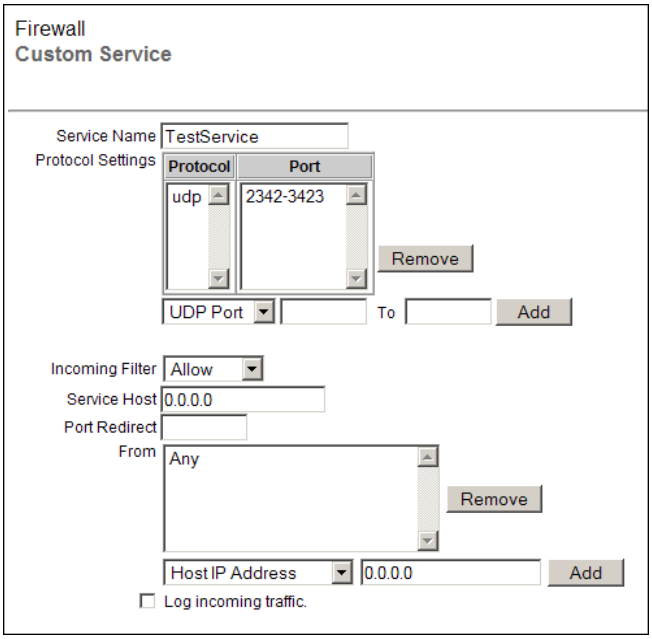
1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Firewall** > **Incoming**.
The Filter Incoming Traffic page appears.

3 Scroll to the bottom of the page.



4 Below **Custom Services**, click **Add Service**.
The Custom Service page appears.



5 In the **Service Name** text box, type the name for your service.

6 From the **Protocol Settings** drop-down list, select **TCP Port**, **UDP Port**, or **Protocol**.

7 In the text box adjacent to the **Port/Protocol** drop-down list, type a port number or protocol number.
To use a single port, type a port number in the first text box.
To use a range of ports, type the lower port number in the first text box, and the higher port number in the second text box.

Note

An IP protocol number is not the same as a TCP or UDP port number. TCP is IP protocol number 6 and UDP is IP protocol number 17. If you use an IP protocol that is not TCP or UDP, you must enter its number. IP protocols numbers include: 47 for GRE (Generic Routing Encapsulation) and 50 for ESP (Encapsulated Security Payload). Most settings are done with TCP or UDP ports.

8 Click **Add**.
Repeat steps 6-8 until you have a list of all the ports and protocols that this service uses. You can add more than one port and more than one protocol to a custom service. More ports and protocols make the network less secure. Add only the ports and protocols that are necessary.

Filter incoming traffic for a custom service

These steps restrict incoming traffic for a service to specified computers behind the firewall. Refer to the subsequent section for information on controlling outgoing traffic.

1 From the **Incoming Filter** drop-down list, select **Allow** or **Deny**.

2 If you set the Incoming Filter to **Allow**, type the IP address of the service host. This is the computer that receives the traffic.
To allow incoming traffic from the external network without restrictions, skip to step 8.

3 If you redirect the service to another port, type the port number in the text box adjacent to **Port Redirect**.
For more information, see "Working with Firewall NAT" on page 97.

4 To limit incoming traffic from the external network to the service host, use the drop-down list to select **Host IP Address**, **Network IP Address**, or **Host Range**.

5 In the address text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the external network that can send traffic to the service host.
Type Network IP addresses in "slash" notation (also known as CIDR or Classless Inter-Domain Routing notation). For more information on entering IP addresses in slash notation, see this FAQ:
http://www.watchguard.com/support/advancedfaqs/general_slash.asp

6 Click **Add**. The **From** box shows the host range, host IP address, or network IP address that you typed.
Repeat steps 3-5 until all of the address information for this custom service is set. The From box can have more than one entry.

7 If this service is only for incoming traffic, keep the outgoing filter set to **No Rule**.
To limit which computers can send information using this service, go to the subsequent section, "Filtering outgoing traffic for services."

8 Click **Submit**.

Filter outgoing traffic for a custom service

These steps restrict outgoing traffic through the Firebox X Edge. Refer to the previous section for information on filtering incoming traffic.

1 From the **Outgoing Filter** drop-down list, select **Allow** or **Deny**.
To allow all outgoing traffic from the trusted or optional network to the external network using this service, skip to step 9.

2 To limit which computers on the trusted or optional network can send traffic to the external network using this service, use the drop-down list below the **From** box to select **Host IP Address**, **Network IP Address**, or **Host Range**.
To only limit which computers receive information, skip to step 5.

3 In the adjacent text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the trusted or optional network that can use this service to send traffic to the external network.
Network IP addresses must be entered in "slash" notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on entering IP addresses in slash notation, see this FAQ:
http://www.watchguard.com/support/advancedfaqs/general_slash.asp.

4 Click **Add**. The **From** box shows the IP addresses you added.
Repeat steps 2-4 until all of the address information for this custom service is set. The From box can have more than one entry.

5 To limit which computers on the external network can receive network traffic with this service, use the drop-down list below the **To** box to select **Host IP Address, Network IP Address,** or **Host Range.**

6 In the adjacent text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the external network that internal computers can connect to using this service.

Network IP addresses must be entered in "slash" notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on entering IP addresses in slash notation, see this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.

7 Click **Add**. The **To** box shows the IP addresses you added.

Repeat steps 5-7 until all of the address information for this custom service is set. The To box can have more than one entry.

8 If this service is only for outgoing traffic, keep the Incoming Filter set to **No Rule**.

To limit which computers can receive information using this service, go to the previous section, "Filter incoming traffic for a custom service" on page 82.

9 Click **Submit**.

Configuring Outgoing Services

You control traffic that starts in the trusted or optional network and goes to the external network using outgoing services. Usually, the Internet is the external network.

By default, the Firebox® X Edge e-Series allows all traffic that starts in the trusted or optional networks to go to the external network. To deny outgoing connections, you must make rules for those connections.

Note

The outgoing services in this section have no effect on traffic between the trusted and optional networks. These services also have no effect on traffic between computers on the trusted network or between computers on the optional network.

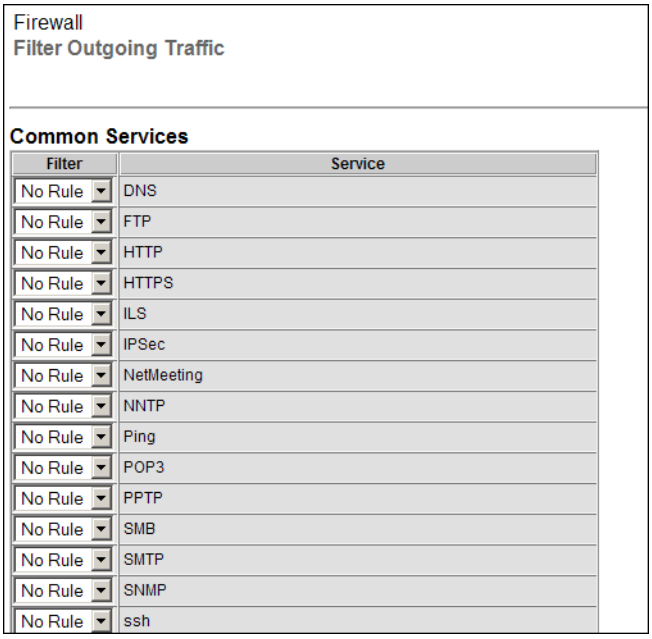
To see the outgoing traffic rules:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.

The default URL is: https://192.168.111.1

2 From the navigation bar, select **Firewall** > **Outgoing**.

The Filter Outgoing Traffic page appears.



Configuring common services for outgoing traffic

By default, the Firebox X Edge allows all traffic to go out to the external network. This is because the common service called Outgoing is set to **Allow**. When the Outgoing common service is set to **Deny**, all outgoing traffic is blocked. When the Outgoing common service is set to **No Rule**, traffic that is not specially permitted is blocked.

The Outgoing common service and other common services are found on the **Firewall > Outgoing** page.

- To allow all traffic from the trusted and optional networks to get to the external network, you must set the Outgoing common service to **Allow**.
- To allow only specified traffic from the trusted and optional network to get to the external network, you must:
  - Set the Outgoing common service to **No Rule**.
  - Select other common services and set them to **Allow**.

Note

To limit traffic sent from the trusted or optional networks not specified in a common service, you must create a custom service.

About custom services for outgoing traffic

A custom service for outgoing traffic is necessary if:

- You must allow outgoing traffic for a service that is not on the common service list.
- You must restrict the IP addresses on the trusted or optional network that can use a service.

You can add a custom service using one or more of these:

- TCP ports

- UDP ports
- An IP protocol that is not TCP or UDP. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

Adding a custom service using the wizard

1 From the navigation bar, click **Wizards**.

2 Adjacent to **Define a custom service**, click **Go**.

3 Follow the instructions in the wizard.

The Traffic Filter Wizard includes these steps:

Welcome
The first screen tells you about the wizard and the information you must have to complete the wizard.

Service Name
Type a name to identify the service.

Protocols and Ports
Set the protocol and ports to assign to this traffic rule.

Traffic Direction
Identify if this is an incoming or outgoing service.

Service action
Configures the Edge to allow or deny this type of service traffic through the firewall.

Restrict to remote computers
To put a limit on the scope of the service, add the IP addresses of the computers or networks outside the firewall to which this service applies.

Restrict to local computers
To put a limit on the scope of the service, add the IP addresses of the computers or networks inside the firewall to which this service applies.

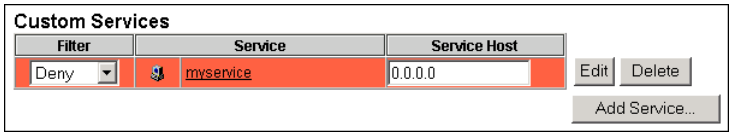
Adding a custom outgoing service manually

You can add a custom service without using the wizard:

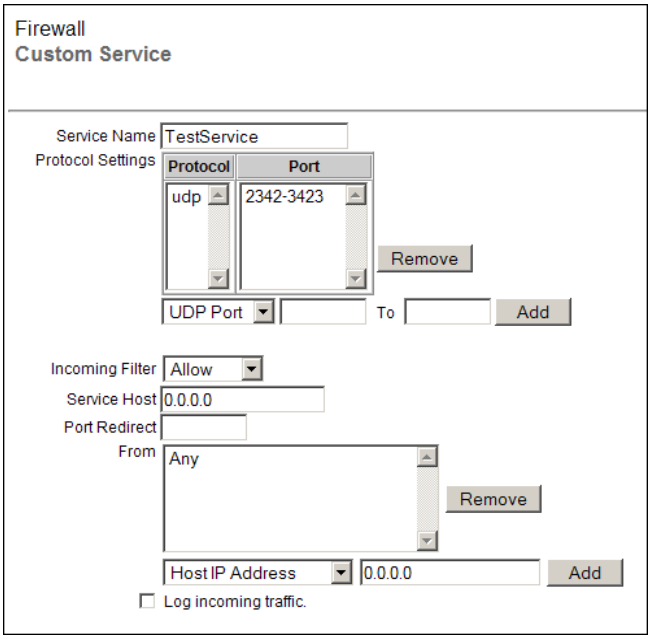
1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Firewall** > **Outgoing**.

3 Scroll to the bottom of the page.



4 Below **Custom Services**, click **Add Service**.
The Custom Service page appears.



5 In the **Service Name** text box, type the name for your service.

6 From the **Protocol** drop-down list, select **TCP Port**, **UDP Port**, or **Protocol**.

7 In the text box adjacent to the **Protocol** drop-down list, type a port number or protocol number. To use a range of ports, type a port number in the second text box.

Note

An IP protocol number is not the same as a TCP or UDP port number. TCP is IP protocol number 6 and UDP is IP protocol number 17. If you use an IP protocol that is not TCP or UDP, you must enter its number. IP protocols numbers include: 47 for GRE (Generic Routing Encapsulation) and 50 for ESP (Encapsulated Security Payload). Most settings are done with TCP or UDP ports.

8 Click **Add**.

Repeat steps 6-8 until you have a list of all the ports and protocols that this service uses. You can add more than one port and more than one protocol to a custom service. More ports and protocols can make the network less secure. Add only the ports and protocols that are necessary.

Filter traffic for an outgoing service

To limit the computers that can send incoming traffic from the external network using the service, see "Filter incoming traffic for a custom service" on page 82. To limit what computers can send traffic from the internal network using the service, and what computers on the external network can receive that traffic, see "Filter outgoing traffic for a custom service" on page 82.

Services for the Optional Network

By default, the Firebox® X Edge e-Series allows all traffic that starts in the trusted network and tries to go to the optional network, and denies all traffic that starts in the optional network and tries to go to the trusted network.

Here are some examples of how you can use the optional network:

- You can use the optional network for servers that the external network can get to. This helps to protect the trusted network, because no traffic is allowed to the trusted network from the optional network when the Firebox X Edge is in default configuration.

When computers are accessible from the external network, they are more vulnerable to attack. If your public web or FTP server on the optional network is hacked or compromised, the attacker cannot get to your trusted network.

- You can use the optional network to secure a wireless network. Wireless networks are usually less secure than wired networks. If you have a wireless access point (WAP), you can increase the security of your trusted network by keeping the WAP on the optional network.
- You can use the optional network to have a different network IP address range that is allowed to communicate with the trusted network. See the section "Disabling Traffic Filters," below.

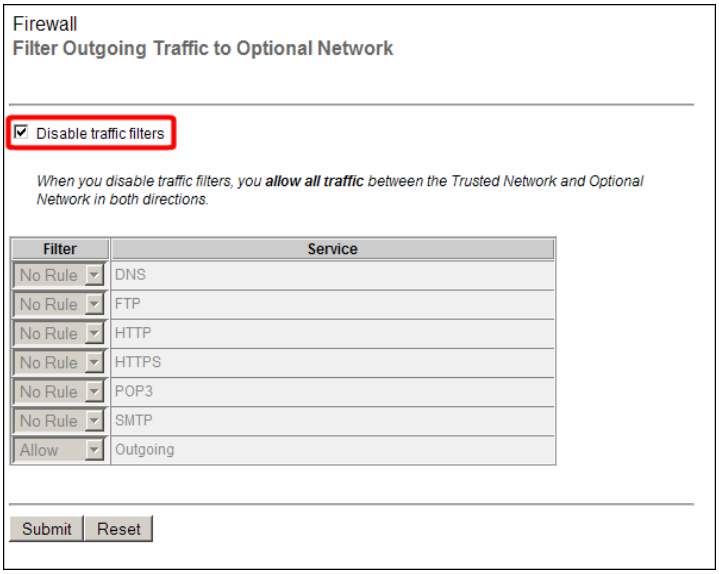
Controlling traffic from the trusted to optional network

Do these steps to deny traffic that goes from the trusted network to the optional network:

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
   The default URL is: https://192.168.111.1
2. From the navigation bar, click **Firewall > Optional**.
   The Filter Outgoing Traffic to Optional Network page appears.
3. To allow all traffic from the trusted network, select **Allow** for the Outgoing service from the **Filter** drop-down list.
4. To deny all traffic from the trusted network, select **Deny** for the Outgoing service from the **Filter** drop-down list.
5. To deny some traffic, but allow all other traffic from the trusted network to the optional network, set the Outgoing service to **Deny** from the **Filter** drop-down list. Then, for each service that is permitted, select **Allow** from the **Filter** drop-down list.
   If you want to deny the traffic and create a log entry for each time the traffic is denied, select No Rule.
6. Click **Submit**.

Disabling traffic filters between trusted and optional networks

To allow network traffic from the optional network to the trusted network, you must allow all traffic between the trusted and optional networks. Select the **Disable traffic filters** check box to allow all incoming and outgoing traffic between the trusted and optional interfaces.



Note

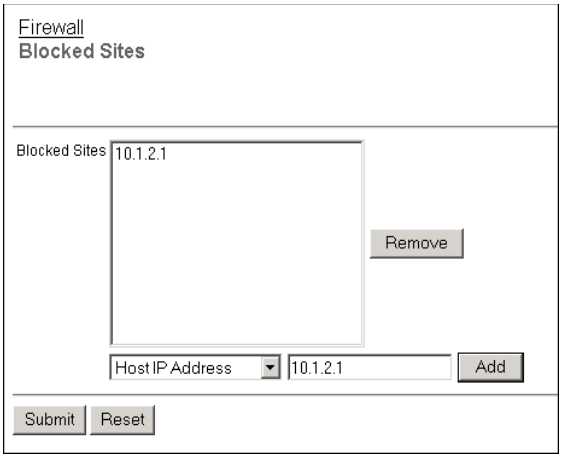
When you select the Disable traffic filters check box, the trusted network is not protected from the optional network. All traffic can flow between the optional and trusted networks.

Blocking External Sites

A Blocked Site is an external IP address that is always blocked from connecting to computers behind the Firebox® X Edge e-Series. You can examine the data in your log files to look for patterns of suspicious actions and identify the IP addresses that start the connections. Use these IP addresses to create a Blocked Sites list.

To add a location to the Blocked Sites list:

1 From the navigation bar, click **Firewall** > **Blocked Sites**.
The Blocked Sites page appears.



2 From the drop-down list, click **Host IP Address**, **Network IP Address**, or **Host Range**.

3 In the text box, type a host IP address, a network IP address, or a range of host IP addresses.

4 Click **Add**.
The IP address information appears in the Blocked Sites list.
Repeat steps 2-4 to add many IP addresses at one time.

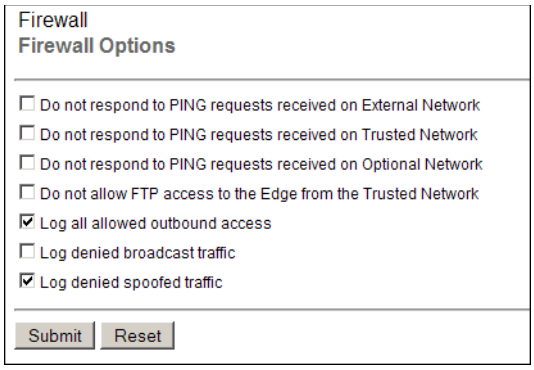
5 Click **Submit**.

Configuring Firewall Options

You can use the Firewall Options page to configure rules that increase your network security.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox® X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **Firewall** > **Firewall Options**.
The Firewall Options page appears.


Firewall
Firewall Options
Do not respond to PING requests received on External Network
Do not respond to PING requests received on Trusted Network
Do not respond to PING requests received on Optional Network
Do not allow FTP access to the Edge from the Trusted Network
Log all allowed outbound access
Log denied broadcast traffic
Log denied spoofed traffic
Submit
Reset

Responding to ping requests

You can configure the Firebox X Edge e-Series to deny ping requests. This option overrides all other Edge settings.

1 Select the **Do not respond to PING requests received on External Network** check box or the **Do not respond to PING requests received on Trusted Network** check box.

2 Click **Submit**.

Denying FTP access to the Firebox X Edge

You can configure the Firebox X Edge e-Series to not allow any FTP connections from the trusted network. This option overrides all other Edge settings.

1 Select the **Do not allow FTP access to the Edge from the Trusted Network** check box.

2 Click **Submit**.

Note

You must clear the **Do not allow FTP access to the Edge from the Trusted Network** check box when you apply an update to the Firebox X Edge firmware with the automatic installer. If you do not clear this check box, the Software Update Installer cannot move firmware files to the Edge.

Logging all allowed outgoing traffic

If you use the standard property settings, the Firebox X Edge e-Series records only unusual events. When traffic is denied, the Edge records the information in the log file. You can configure the Edge to record information about all the outgoing traffic in the log file.

Note

Recording all outgoing traffic creates a large number of log records. We recommend that you record all the outgoing traffic only as a problem-solving tool, unless you send log messages to a remote Log Server. For more information, see “Viewing Log Messages” on page 103.

To record all outgoing traffic:

1 Select the **Log all allowed outbound access** check box.

2 Click **Submit**.

Logging denied broadcast traffic

If you use the standard property settings, the Firebox X Edge e-Series records only unusual events. When traffic is denied, the Edge records the information in the log file. You can configure the Edge to record information about denied network traffic that was sent to many destinations at the same time.

To record denied broadcast traffic:

1 Select the **Log denied broadcast traffic** check box.

2 Click **Submit**.

Log denied spoofed traffic

If you use the standard property settings, the Firebox X Edge e-Series records only unusual events. When traffic is denied, the Edge records the information in the log file. You can configure the Edge to record information when the source IP address of network traffic does not match the IP address of the host that sent the traffic.

To record denied spoofed traffic:

1 Select the **Log denied spoofed traffic** check box.

2 Click **Submit**.

Changing the MAC address of the external interface

Some ISPs use a MAC address to identify the computers on their network. Each MAC address gets one static IP address. If your ISP uses this method to identify your computer, then you must change the MAC address of the Firebox X Edge external interface. Use the MAC address of the cable modem, DSL modem, or router that connected directly to the ISP in your original configuration.

The MAC address must have these properties:

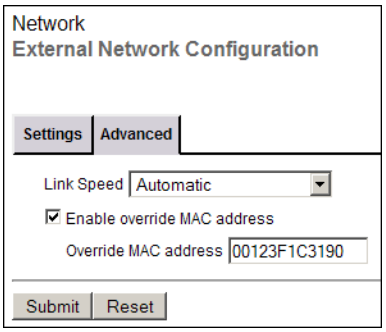
- The MAC address must use 12 hexadecimal characters. Hexadecimal characters have a value between 0 and 9 or between “a” and “f.”
- The MAC address must operate with:
  - One or more addresses on the external network
  - The MAC address of the trusted network for the Firebox X Edge
  - The MAC address of the optional network for the The Firebox X Edge
- You cannot set the MAC address to 000000000000 or ffffffffffff

To change the MAC address of the external interface:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **Network > External**.
The External Network Configuration page appears.

3 Below the **Advanced** tab, select the **Enable override MAC address** check box.



4 In the **Override MAC address** text box, type the new MAC address for the Firebox X Edge external network.

You must enter the MAC address as a hexadecimal number.
Do not use extra characters, such as spaces or hyphens.

5 Click **Submit**.

You must restart the Firebox to see the changes.

Note

If the **Override MAC address** field is cleared and the Firebox X Edge is restarted, the Firebox X Edge uses the default MAC address for the external network.

To decrease problems with MAC addresses, the Firebox X Edge makes sure that the MAC address you assign to the external interface is unique on your network. If the Edge finds a device using the same MAC address, the Firebox changes back to the standard MAC address for the external interface and restarts again.

CHAPTER 8

Managing Network Traffic

The Firebox® X Edge e-Series allows many different ways to manage the traffic on your network. You can limit the rate of traffic sent to the external interface using QoS (Quality of Service) through Traffic Control. You can manage data transmission by giving more or less bandwidth to different traffic types. You can also change the apparent network address of incoming or outgoing traffic to prevent conflicts using NAT (Network Address Translation).

About Network Traffic

Bandwidth is the quantity of data that can be sent through the network in a specified increment of time. It is usually expressed in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps). A T1 line supplies approximately 1.5 Mbps, while a dial-up connection supplies approximately 56 Kbps. Latency is the quantity of time necessary for a packet to go from a source to a destination.

Together, latency and bandwidth define the speed and capacity of a network. You can improve latency by configuring Traffic Control. You must upgrade your Internet connection with your ISP to improve bandwidth.

When too many users or devices try to send data at the same time, the Firebox® X Edge cannot send all of the data quickly. When the Edge has more traffic than the external connection can send at the same time, some programs appear to operate slowly.

Causes for slow network traffic

Many programs use as much bandwidth as possible to operate. If too many users operate these programs, other users cannot use the network. Peer-to-peer (P2P) services, instant messaging, and file downloads are programs that frequently use large quantities of bandwidth.

To limit the quantity of bandwidth those software applications can use, you must use Traffic Control. To deny or allow traffic from those software applications, you must configure a service. For more information on services, see Chapter 7, “Configuring Firewall Settings”.

Traffic Categories

The Firebox® X Edge e-Series allows you to limit data sent through services and Traffic Control filters. A service can allow or deny all data of a specified type. Traffic Control does not allow or deny data, but creates "filters" that separate important network traffic from other data. For example, you can create a filter that identifies e-mail (SMTP) traffic or secure shell (SSH) connections.

When you create a filter, you must select the priority for the traffic it identifies. There are four categories of network traffic: interactive, high, medium, and low. You can create as many as 100 traffic filters in each traffic category. Filters can be based on the IP protocol type, the source or destination IP address, and the source or destination port.

Interactive traffic is routed before all other traffic. Bandwidth not used for interactive traffic is divided between high, medium, and low priority traffic. Unused bandwidth is automatically given to other categories. For example, if there is no interactive or low priority traffic, all of the bandwidth is divided between high and medium priority traffic.

Interactive traffic

Interactive traffic is sent before any other traffic and is only limited by the speed of your connection. Use the interactive category for traffic that must have low latency. Some examples of interactive traffic are Telnet, Secure Shell (SSH), video communication, and Voice over Internet Protocol (VoIP).

High priority

High priority traffic is given 75% of the bandwidth not used by interactive traffic. Use the high priority category for traffic that is very important to your company or uses a lot of bandwidth. Some examples of high priority traffic are secure HTTP (HTTPS) and virtual private network (VPN) traffic.

Medium priority

Medium priority traffic is given 20% of the bandwidth not used by interactive traffic. When traffic control is enabled, any traffic that is not in a different filter is automatically put in the medium category. This traffic is represented by the "All other traffic" entry on the Traffic Control page.

Low priority

Low priority traffic is given 5% of the bandwidth not used by interactive traffic. Use the low priority category for low priority traffic that does not use much bandwidth, or is not important. Some examples of low priority traffic are peer-to-peer (P2P) file transfers or instant messaging (IM).

Configuring Traffic Control

The Firebox® X Edge e-Series has three traffic control options:

Traffic control is off
: The Edge sends network traffic in the sequence it was received.

Traffic control is on, but prioritization is off
: This option limits all traffic to the upstream bandwidth limit.

Traffic control and prioritization are on

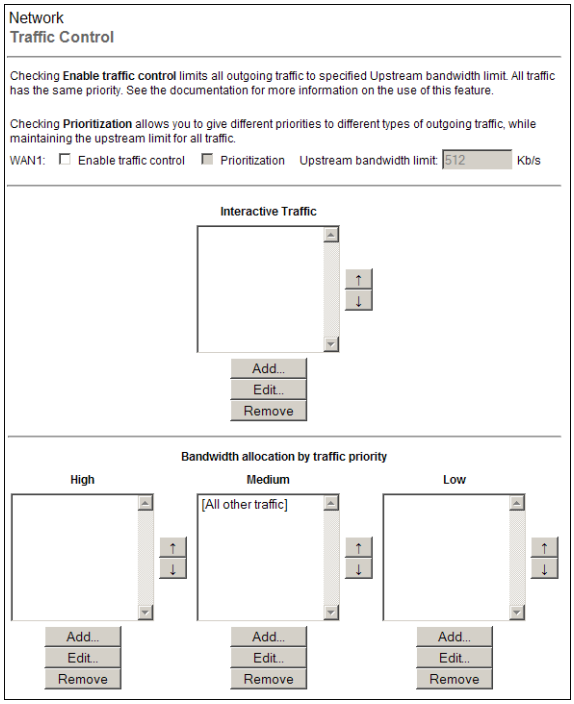
This option allows you to configure filters for all traffic categories.

Note

To use prioritization, you must know your upstream bandwidth limit in kilobits per second (Kb/s). If you do not know your upstream bandwidth limit, ask your network administrator or ISP. For better traffic control, the Edge subtracts 5% from the upstream bandwidth rate limit to decrease packet latency. If you enter an incorrect upstream bandwidth limit, traffic control does not operate correctly.

Enable traffic control

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
   The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Network > Traffic Control**.
   The Traffic Control page appears.


Network
Traffic Control
Checking Enable traffic control limits all outgoing traffic to specified Upstream bandwidth limit. All traffic has the same priority. See the documentation for more information on the use of this feature.
Checking Prioritization allows you to give different priorities to different types of outgoing traffic, while maintaining the upstream limit for all traffic.
WAN1: Enable traffic control Prioritization Upstream bandwidth limit: 512 Kb/s
Interactive Traffic
Add...
Edit...
Remove
Bandwidth allocation by traffic priority
High
Medium
Low
[All other traffic]
Add...
Edit...
Remove

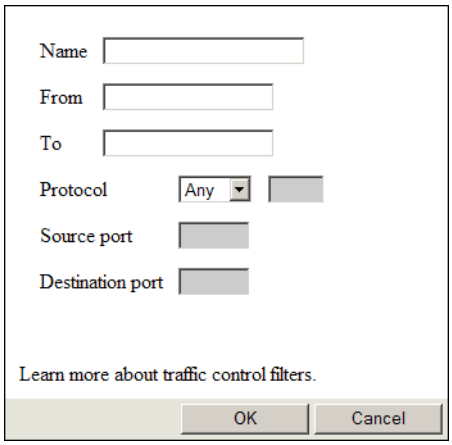
3. Select the **Enable Traffic Control** check box.
   The Interactive traffic list is enabled.
4. In the **Upstream bandwidth limit** text box, type the upstream bandwidth limit of your external network connection (WAN1).
   Enter a value from 19 Kbps to 100,000 Kb/s. The default setting is 512 Kb/s.
5. Select the **Prioritization** check box if you want to add filters to the other categories.
   The prioritization lists are enabled.
6. To create filters for the interactive, high, medium, or low traffic categories, click the **Add** button adjacent to the category name. To change a filter, click **Edit**. To delete a filter, click **Remove**.
   For instructions on how to add, edit, or remove a traffic filter, see the subsequent sections.

7 Click **Submit**.
Traffic control is enabled.

Add a traffic control filter

Before you add a traffic control filter to allow or deny traffic for an program, you must know the port numbers that the program uses to send data. If you do not know the port numbers, see the documentation for the program.

1 Click the **Add** button adjacent to the traffic category.
The Add Traffic Control dialog box appears.



2 In the **Name** text box, type a name for the traffic control filter.
This name is used on the Traffic Control page to identify the filter.

3 In the **From** text box, type the IP address or subnet of the traffic source or local network associated with this filter.

You can type an IP address (192.168.111.13), a subnet address in slash notation (192.168.111.0/24), or a host address in CIDR notation (192.168.111.2/32).
If this text box is empty, the filter applies to any source address.
For more information, see “Making Static Routes” on page 57.

4 In the **To** text box, type the IP address or subnet of the traffic destination or remote network associated with this filter.

You can type an IP address (192.168.111.13), a subnet address in slash notation (192.168.111.0/24), or a host address in CIDR notation (192.168.111.2/32).
If this text box is empty, the filter applies to any destination address.
For more information, see “Making Static Routes” on page 57.

5 From the **Protocol** drop-down list, select the IP protocol for traffic associated with this filter.
If you select "Other," you must enter a valid IP protocol number in the adjacent text box.
The range for IP protocols is 1 to 255.

6 In the **Source port** text box, type the source port for traffic associated with this filter.
This field is enabled only when the protocol is TCP or UDP.
You can enter a value from 1 to 65535. If you do not enter a number, all ports are used.

7 In the **Destination port** text box, type the destination port for traffic associated with this filter.
This field is enabled only when the protocol is TCP or UDP.
You can enter a value from 1 to 65535. If you do not enter a number, all ports are used.

8 Click **OK** to add the filter to the category.

9 Click **Submit** on the Traffic Control page to save your changes.

Edit a traffic control filter

1 Select one entry from any category, then click the **Edit** button adjacent to the category.
The Edit Traffic Control Filter dialog appears.
2 Complete the fields as shown in the procedure, "Add a traffic control filter".
3 Click **Submit** on the Traffic Control page to save your changes.

Change the priority of a traffic control filter

1 Select an entry from any category.
To select multiple entries, hold down the Control or Shift key.
2 To make the traffic more important, click the **Up** button adjacent to the category list. To make the traffic less important, click the **Down** button.
The entries move to the new position in the list.
3 Click **Submit** on the Traffic Control page to save your changes.

Remove a traffic control filter

1 Select one entry from any category, then click **Delete**.
The entry is removed from the traffic control category.
2 Click **Submit** on the Traffic Control page to save your changes.

Working with Firewall NAT

The Firebox® X Edge e-Series supplies advanced NAT (Network Address Translation) options. NAT was first developed as a solution for organizations that could not get a sufficient quantity of registered IP network numbers for their needs.

NAT can refer to many different types of IP address and port translation. Each type of NAT allows many devices to use the same IP address at the same time to send data to a different network. NAT is also used to hide the private IP addresses of hosts on your LAN. When you use NAT, the source IP address is changed on all of the packets you send.

NAT types

The Firebox X Edge supports three different forms of NAT. Many users use more than one type of NAT at the same time. You apply some types of NAT to all firewall traffic, and other types as a setting in a policy.

Dynamic NAT

Dynamic NAT, also known as "IP masquerading," changes the source port and source IP address for outgoing connections. The source IP address is changed to the external IP address of the Firebox X Edge. This hides the real IP address of the host that sends the packet from the external network. Dynamic NAT is frequently used to hide the IP addresses of trusted and optional hosts when they get access to public services.

The Edge automatically uses Dynamic NAT on all outgoing traffic. If you want outgoing traffic from a host on the trusted or optional network to show an IP address that is different from the primary IP address on the external interface, you must use 1-to-1 NAT.

1-to-1 NAT

When you enable 1-to-1 NAT, the Firebox X Edge e-Series changes all incoming and outgoing packets sent from one IP address to a different IP address. 1-to-1 NAT is frequently used when you have an internal server with a private IP address that must be made public. You can use 1-to-1 NAT to map a secondary external IP address to the server behind the Edge. You do not have to change the IP address of your internal server.

Static NAT

Static NAT is also known as "port forwarding." When you use static NAT, you use the primary external IP address of your Firebox X Edge e-Series instead of the IP address of a public server. You could do this because you want to, or because your public server does not have a public IP address.. Traffic to that internal server is sent to a port on the public IP address of your Firebox X Edge. The Edge uses Static NAT to send the traffic on that port to the server behind the Edge.

For example, you can put your SMTP e-mail server behind the Edge with a private IP address and configure static NAT in your SMTP policy. The Firebox X Edge receives connections on port 25 and makes sure that any SMTP traffic is sent to the real SMTP server behind the Edge.

You configure Static NAT with incoming firewall services. For more information, see "Configuring common services for incoming traffic" on page 79.

NAT behavior

When you configure NAT:

1. Each interface on the Firebox X Edge e-Series must use a different TCP subnet.
2. There can only be one trusted network, one optional network, and one external network.
   You can use a router to connect more subnets to these networks. For more information, see "Connecting the Edge to more than four devices" on page 15.
3. The Edge always uses Dynamic NAT for traffic going from the trusted or optional networks to the external network.
4. Dynamic NAT is not applied to BOVPN or MUVPN traffic.

Secondary IP addresses

You can assign eight public IP addresses to the primary external interface (WAN1). These addresses are used for 1-to-1 NAT.

When you configure secondary IP addresses on the external network:

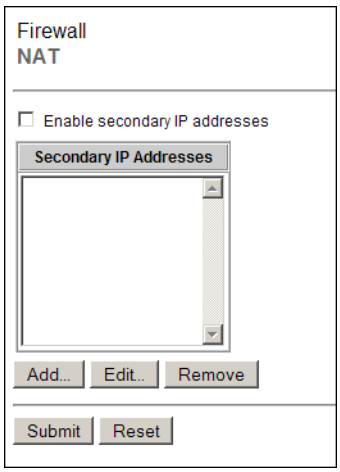
1. The primary IP address must be a static IP address.
   The first IP address is the primary IP address.
2. All secondary IP addresses must be on the same external subnet as the primary IP address.
3. You cannot configure multiple IP addresses for the WAN2 failover interface.
   The WAN2 interface is reserved for WAN failover, and your failover IP address must be on a different subnet.

Enable 1-to-1 NAT

Note

You must add at least one 1-to-1 NAT entry before you can enable 1-to-1 NAT. For more information, see the subsequent section.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
   The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Firewall > NAT**.
   The NAT (Network Address Translation) page appears.



3. Select the **Enable secondary IP addresses** check box.
4. Click **Submit**.

Add a 1-to-1 NAT entry

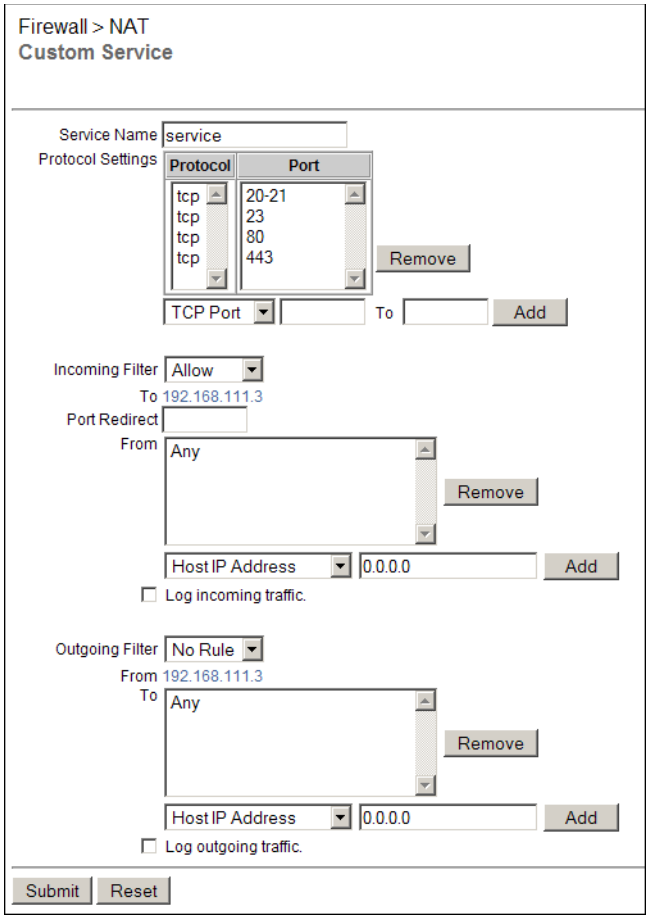
1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
   The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Firewall > NAT**.
   The NAT (Network Address Translation) page appears.
3. Click **Add**.
   The Mapping page appears.

4. In the **Public Address** text box, type a secondary external IP address.
   The address must be on the external network subnet.
5. In the **Private Address** text box, type a private IP address from the trusted or optional network.
   The Firebox X Edge maps the private IP address you type here to the secondary external IP address.
6. Click **Submit**.
   The entry is added to the Secondary IP Addresses list.

7 To add a custom service to the NAT entry, click **Add Service**.
For more information, see the subsequent section.

Add or Edit a Custom Service for 1-to-1 NAT

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2 From the navigation bar, select **Firewall > NAT**.
The NAT (Network Address Translation) page appears.
3 Select the 1-to-1 NAT entry you want to edit, then click **Edit**.
The Custom Service page appears.



4 In the **Service Name** text box, type a name for the service.
5 Under **Protocol Settings**, select the protocol type.
You can select TCP port, UDP port, or Protocol.
6 Adjacent to the **Protocol Settings** drop-down list, type a TCP or UDP port range in the text boxes, or a protocol number in the text box.
7 From the **Incoming Filter** drop-down list, select **Allow** to let incoming traffic reach the host, **Deny** to prevent incoming traffic, or **No Rule** to use the default settings.
If you select No Rule, all incoming traffic is blocked by default.
8 To redirect the traffic coming to this IP address to a specific port, type a port number in the **Port Redirect** text box.

9 To add a host or network to the **From** list, select Host IP Address, Network IP Address, or Network Range from the drop-down list. Type the IP address or range in the adjacent text box and click **Add**.
The entry is added to the From list. To remove an entry, select an IP address or range and click Remove.

10 To create an entry in the log for each incoming packet, select the **Log Incoming Traffic** check box.

11 From the **Outgoing Filter** drop-down list, select **Allow** to let outgoing traffic go from the host, **Deny** to prevent outgoing traffic, or **No Rule** to use the default settings.
If you select No Rule, all outgoing traffic is blocked by default.

12 To add a host or network to the **To** list, select Host IP Address, Network IP Address, or Network Range from the drop-down list. Type the IP address or range in the adjacent text box and click **Add**.
The entry is added to the To list. To remove an entry, select an IP address or range and click Remove.

13 To create an entry in the log for each outgoing packet, select the **Log Outgoing Traffic** check box.

14 Click **Submit**.
The custom service settings are saved.

Remove a 1-to-1 NAT entry

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`

2 From the navigation bar, select **Firewall > NAT**.
The NAT (Network Address Translation) page appears.

3 Select the 1-to-1 NAT entry you want to delete, then click **Remove**.
The entry is removed from the Secondary IP Addresses list.

CHAPTER 9

Configuring Logging and System Time

A log file is a list of all the events that occur on the Firebox® X Edge e-Series. A log file records and saves information about these events.

A log message is an important part of a network security policy. A sequence of denied packets can show a pattern of suspicious network activity. Log records can help you identify possible security problems.

Note

The Firebox X Edge log is cleared if the power supply is disconnected or the Edge is restarted. To keep the information permanently, you must configure an external syslog or Log Server.

Viewing Log Messages

The Firebox® X Edge e-Series uses up to 640KB of memory for log messages. New information shows at the top of the file. When new information enters a full log file, it erases the log message at the bottom of the file.

Each log message contains this information:

Time
The time of the event that created the log message.

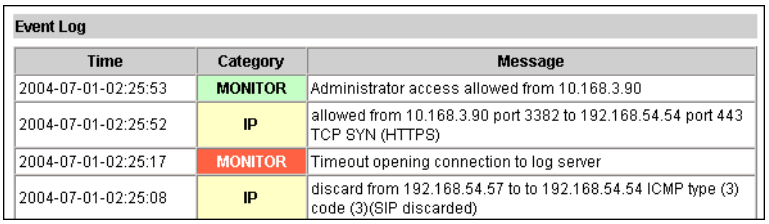
Category
The type of message. For example, if the message came from an IP address or from a configuration file.

Message
The text of the message.

Use this procedure to see the event log file:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **Logging**.
The Logging page appears with the Event Log at the bottom of the page.

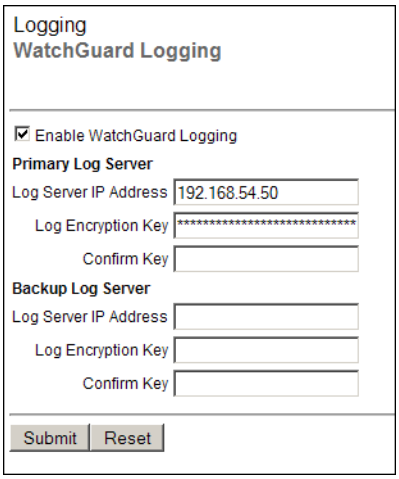


Log to a WatchGuard Log Server

The WatchGuard® Log Server (previously known as the WatchGuard System Event Processor, or WSEP) is a component of the WatchGuard System Manager. If you have a Firebox® III, Firebox X Core, or Firebox X Peak, configure a primary Log Server to collect the log messages from your Firebox X Edge e-Series. You also can configure a backup Log Server. If the Firebox X Edge cannot connect to the primary Log Server, it tries to connect to the backup Log Server. It sends log messages to the backup Log Server until the primary Log Server becomes available. When the Firebox X Edge can resume its connection to the primary Log Server, it automatically starts to send log messages to the primary Log Server again. For instructions on how to configure the Log Server to accept log messages, see the WatchGuard System Manager User Guide. Use these instructions to send your event logs to the Log Server.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **Logging** > **WatchGuard Logging.**
The WatchGuard Logging page appears.



3 Select the **Enable WatchGuard Logging** check box.

4 In the **Device Name** field, type a name for the Firebox X Edge.
This name lets the Log Server know which log messages come from which device. The Device Name appears in the Log Viewer. If this field is clear, the Firebox X Edge is identified in the log by the IP address of the Edge external interface.

5 Below Primary Log Host, type the IP address of the primary Log Server in the **Log Host IP Address** field.

6 Type a passphrase in the **Log Encryption Key** field and confirm the passphrase in the **Confirm Key** field.
The same passphrase also must be used when the Log Server is configured to receive log messages from this Firebox X Edge.

7 If you have a backup Log Server available, type its IP address and Log Encryption Key.
If the Firebox X Edge cannot connect to the primary Log Server, it will send log messages to the backup Log Server until the primary Log Server becomes available again.

8 Click **Submit**.

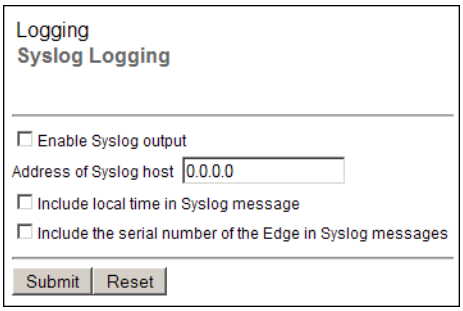
Logging to a Syslog Host

Syslog is a log interface developed for UNIX but also used by a number of computer systems. This option sends the Firebox® X Edge e-Series log messages to a syslog host. If you use a syslog host, you can set the Edge to send log messages to that host.

Follow these instructions to configure a syslog host:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **Logging > Syslog Logging**.
The Syslog Logging page appears.



3 Select the **Enable Syslog output** check box.

4 Adjacent to **Address of Syslog host**, type the IP address of the syslog host.

5 To include the local time in the syslog messages, select the **Include local time in syslog message** check box.

6 To include the Firebox X Edge serial number in the syslog messages, select the **Include serial number in syslog messages** check box.
This setting is useful if you have more than one Firebox X Edge sending syslog messages to the same syslog host.

7 Click **Submit**.

Note

Because syslog traffic is not encrypted, syslog messages that are sent through the Internet decrease the security of the trusted network. Use a VPN tunnel to increase the security of syslog message traffic. If the syslog messages go through a VPN tunnel, IPSec technology encrypts the data.

CHAPTER 10

Managing Users and Groups

The Firebox® X Edge e-Series includes tools you can use to manage your network and your users. You can create users and manage access to the Internet or to your VPN tunnels with user authentication. Or, you can allow free access to the Internet and VPN tunnels to all users. In this chapter, you learn to do these tasks:

- Examine current users and properties
- Configure local Firebox X Edge authentication
- Configure the Edge to use LDAP or Active Directory authentication
- Allow internal hosts to bypass user authentication

Seeing Current Sessions and Users

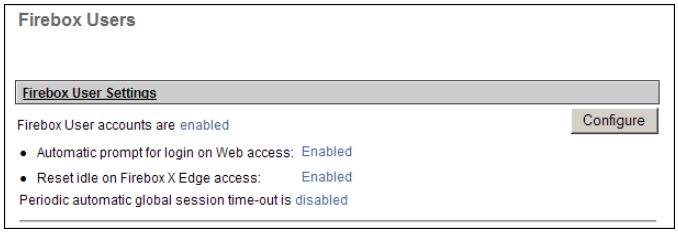
On the Firebox Users page, you see information about the users who are online.

1 To connect to the System Status page, type `https://` in the browser address bar, with the IP address of the Firebox® X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

Firebox Users Settings

Below **Firebox Users Settings**, you can see the current values for all global user and session settings. To see the configuration page for these settings, click the **Configure** button. For more information, see "Using Local Firebox Authentication" on page 113 and "Configuring MUVPN client settings" on page 112.


Firebox Users
Firebox User Settings
Firebox User accounts are enabled
Configure
Automatic prompt for login on Web access: Enabled
Reset idle on Firebox X Edge access: Enabled
Periodic automatic global session time-out is disabled

Active Sessions

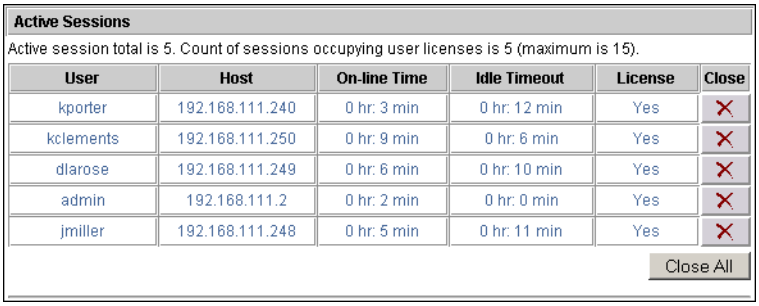
A session is created when traffic goes from a computer on the trusted or optional network to a computer on the external network. For example, when a user on your trusted network opens a browser to connect to a web site on the Internet, a session starts on the Firebox® X Edge.

Note

Only sessions from computers on the trusted or optional network to computers on the external network use a user license. For more information on sessions, see "About session licenses" on page 16.

If local user accounts are enabled, the **Active Sessions** section of the Firebox Users page shows information for all current sessions, including:

- The number of active sessions, licenses used, and total licenses
- The name and IP address of the user who started the session
- The total time since the session started
- The time between the last packet and the session expiration (known as the idle time.)
- Whether the session uses a license



If local user accounts are not enabled, each active session shows the IP address of the hosts that have started sessions. The user name shown is "Anonymous."

Stopping a session

The Firebox X Edge e-Series monitors and records the properties of each user session.

If the Automatic Session Termination time limit for all sessions is reached, or if the Firebox X Edge restarts, all sessions are stopped at the same time. The Edge administrator also can use the Firebox Users page to stop a session.

To stop a session manually:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

3 In the **Active Sessions** list, click the **Close** button adjacent to the session you want to stop. To stop all sessions, click the **Close All** button.

If user authentication is enabled for external network connections, a session stops when one of these events occurs:

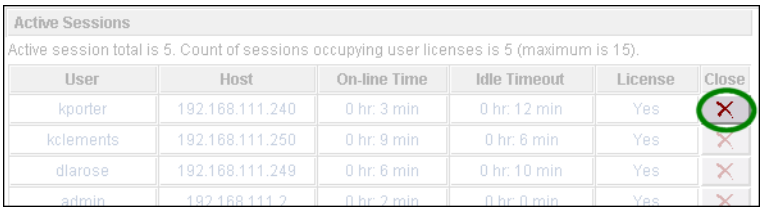
- The idle time-out limit set for that account is reached.
- The maximum time limit set for that account is reached.

- The authenticated user manually stops the session.
  To stop the session, the user clicks the **Logout** button on the Login Status dialog box and closes all open browser windows.

You can increase the number of sessions available with a license upgrade. For more information, see the FAQ:

https://www.watchguard.com/support/AdvancedFaqs/edge_seatlicense.asp

License upgrades are available from your reseller or from the WatchGuard® web site:
http://www.watchguard.com/products/purchaseoptions.asp

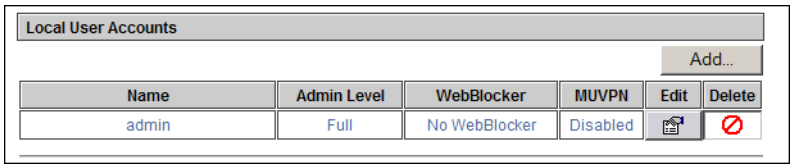


If a session used a user license and the session closes, the user license is available for a different user. For more information on user licenses, see "About User Licenses" on page 110.

Local User Accounts

Below **Local User Accounts**, you can see information on the users you configured:

- **Name:** The name given to the user. The Admin user is part of the default configuration and cannot be deleted.
- **Admin Level**: You can set the user permissions to Full, None, or Read-only. For more information, see "Using Local Firebox Authentication," on page 113.
- **Options**: You can configure a user to use WebBlocker or MUVPN.



If local user accounts are enabled, you also see information about Internet and VPN access rights.

Editing a user account

To edit a user account, click the **Edit** icon. For descriptions of the fields you can configure, see "Using Local Firebox Authentication," on page 113.

Deleting a user account

To remove a user account, click the **X** adjacent to the account name. A dialog box appears. Click **Yes** to remove the account. You cannot delete the "admin" account.

About User Licenses

The Firebox® X Edge e-Series comes with a set number of available user licenses. The number of user licenses puts a limit on how many users can access the Internet at one time. The total number of available user licenses is set by the Edge model you have and any upgrade licenses you apply.

The Firebox Users page shows the maximum number of user licenses available and how many are in use at a given time. You use a user license when you send traffic from the trusted or optional network to the external network.

You do not use a user license when you make connections between computers on the trusted network or through a VPN tunnel. You also do not use a user license when you make connections from the trusted network to the optional network, or connections between computers on the optional network.

If you make users authenticate before they connect to the external network, you can make sure that no user licenses are used by unauthorized computers. If authentication is required, and a user or computer tries to connect to the external network without authenticating, the Firebox X Edge does not allow the connection.

About User Authentication

The Firebox® X Edge e-Series uses advanced authentication options to increase network security. You can configure the Edge as a local authentication server. You can also configure the Edge to use an existing Active Directory or LDAP authentication server. When you use LDAP authentication, account privileges for users that authenticate to the Active Directory/LDAP server are based on group membership.

User authentication gives options to prevent connections to some resources and to help decrease the number of user licenses necessary. This section gives information on how a user can authenticate to the Firebox X Edge, how your users and administrators can close an active session, and which options are available to customize authentication.

Three levels of Administrative Access are available for the Firebox X Edge:

- **None**: Use this to connect to resources on the external network. A user who uses this access level cannot see or change the Edge configuration pages.
- **Read-Only:** Use this to see Edge configuration properties and status. A user who uses this access level cannot change the configuration file.
- **Full**: Use this to see and to change Edge configuration properties. You also can activate options, disconnect active sessions, restart the Edge, and add or edit user accounts. A user who uses this access level can change the passphrase for all user accounts.

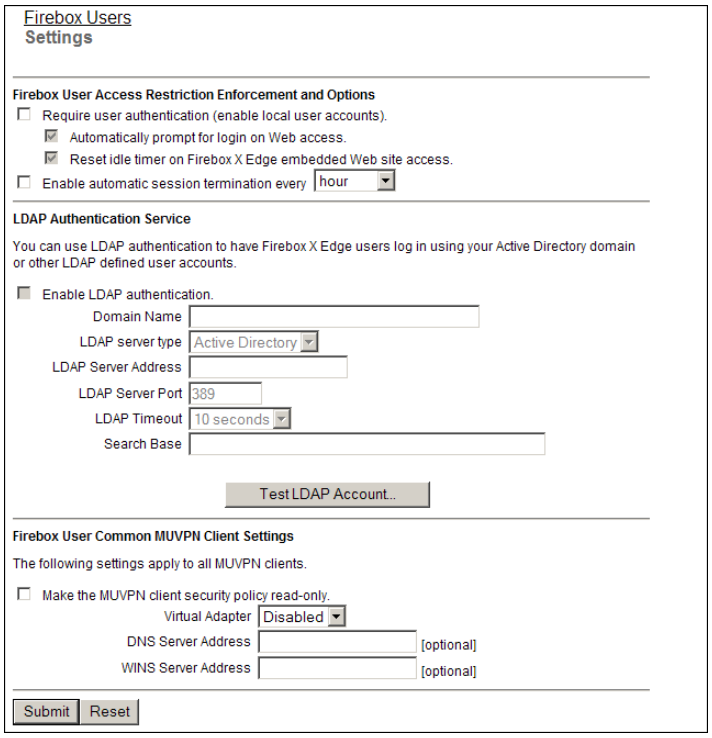
Setting authentication options for all users

Some authentication options have an effect on all users. To set or change authentication options:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **Firebox Users > Settings**.
The Settings page appears.

3 Use the definitions below to help you change your parameters. Click **Submit**.


Firebox Users
Settings
Firebox User Access Restriction Enforcement and Options
Require user authentication (enable local user accounts).
Automatically prompt for login on Web access.
Reset idle timer on Firebox X Edge embedded Web site access.
Enable automatic session termination every
hour
LDAP Authentication Service
You can use LDAP authentication to have Firebox X Edge users log in using your Active Directory domain or other LDAP defined user accounts.
Enable LDAP authentication.
Domain Name
LDAP server type
Active Directory
LDAP Server Address
LDAP Server Port
389
LDAP Timeout
10 seconds
Search Base
Test LDAP Account...
Firebox User Common MUVPN Client Settings
The following settings apply to all MUVPN clients.
Make the MUVPN client security policy read-only.
Virtual Adapter
Disabled
DNS Server Address
[optional]
WINS Server Address
[optional]
Submit
Reset

- **Require User Authentication (Enable local user accounts):** When you select this check box, all hosts must authenticate to the Firebox X Edge to send or receive network traffic. If you do not select this check box, there is no user-based control for access to the Internet or VPN tunnels.

Note

If you configure an incoming service and you enable Firebox User accounts, you must add the servers that accept incoming connections to the Trusted Hosts list.
For more information, see "Allowing Internal Hosts to Bypass User Authentication" on page 120.

- **Automatically prompt for login on Web access**: When you select this check box, the authentication dialog box launches any time a user who has not yet authenticated tries to get access to the Internet.
- **Reset Idle Timer on Embedded Web Site Access**: When you select this check box, the Firebox X Edge does not disconnect a session when an idle time-out occurs if the **Login Status** dialog box is on the desktop. Disable this check box to override the **Login Status** dialog box.

The Login Status box sends traffic to the Firebox X Edge from the user's computer each two minutes. If you enable this check box, the Edge resets the idle timer to zero each time the Edge receives traffic from the Login Status box.

- **Automatic Session Termination** – This is a global property that applies to all sessions and overrides all other authentication options. It lets you clear the list of sessions in use and make all user licenses available again. Enable this check box to disconnect all sessions at the specified time in the drop-down list.

All sessions are disconnected at the same time. The time limit is the number of hours since the Firebox X Edge first starts up, not the length of time a session has been active.

Configuring MUVPN client settings

The MUVPN client settings apply to all MUVPN connections to the Firebox X Edge e-Series. To configure MUVPN client settings:

1 Use your browser to connect to the System Status page. From the navigation bar, select **Firebox Users > Settings**.
The Settings page appears.

2 If necessary, use the scroll bar to scroll to the **Firebox User Common MUVPN Client Settings** section.

3 You can lock the MUVPN client security policy (.wgx file) to prevent accidental changes. Select the **Make the MUVPN client security policy read-only** check box.

4 The remote MUVPN computers can use a virtual adapter to get network settings, an IP address, and WINS and DNS address assignments. You can set the virtual adapter rule for your mobile users to:

Disabled
The mobile user does not use a virtual adapter to connect with the MUVPN client. This is the default value.

Preferred
If the virtual adapter is in use or is not available, the mobile user does not use a virtual adapter to connect with the MUVPN client.

Required
The mobile user must use a virtual adapter to connect with the MUVPN client.

5 You also can enter a WINS Server address and DNS Server address. Type the server IP addresses in the related field.
For more information on configuring the Mobile User VPN client computer, see "Configuring the MUVPN Client" on page 145.

Authenticating to the Edge

When you authenticate with the Firebox X Edge e-Series, it automatically identifies your Administrative Access level. If you select the **Automatically prompt for login on Web access** option from **Firebox Users > Settings**, users see the login dialog box when they open their web browser. If you select this option or not, you can always open the authentication login dialog box with this procedure:

1 Open a web browser.
You can use Netscape Navigator or Microsoft Internet Explorer. It is possible to use the Firebox X Edge with other Web browsers that support Java script, but we do not support them.

2 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

3 A security dialog box appears. You must accept the warning before you can continue.

Note

If your web browser is configured to block pop-up windows, it is possible that some dialog boxes used by the Firebox X Edge will not appear. This includes dialog boxes used by wizards, and the dialog box used to log in to the Edge.

When you authenticate with the Firebox X Edge e-Series, one of two screens appears. A user with Read-Only or Full Administrative Access sees the Edge System Status page. A user with Administrative Access set to None sees a dialog box with an authentication status message. This dialog box is known as the Login Status dialog box.

If you are using local authentication, you must type your name as it appears in the Firebox user list. If you use Active Directory or another LDAP server for authentication through the Firebox X Edge, you must include the domain name. For example, if a user authenticates using the local Firebox user list,he or she types `jsmith`. If the admin user authenticates with an LDAP authentication server through the Edge, the administrator must type `MyCompany\jsmith`.

When you authenticate with the Firebox X Edge and make an Internet connection, your user name appears in the **Active Sessions** section of the Firebox Users page.

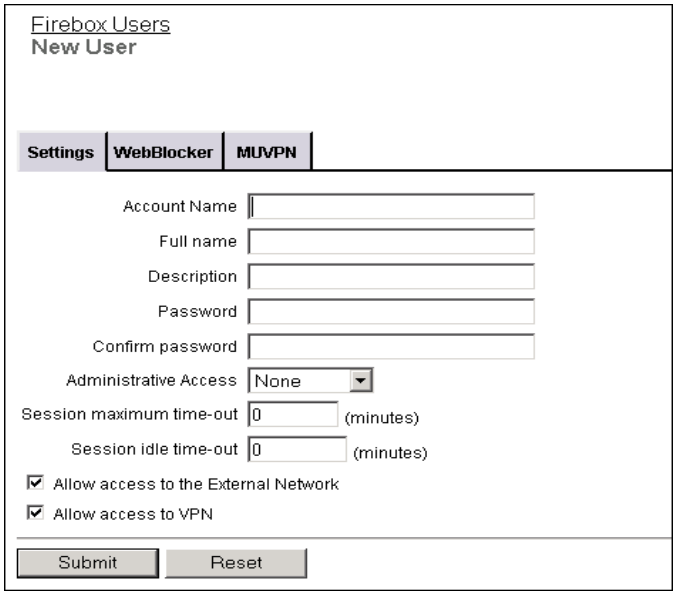
Using Local Firebox Authentication

When you create a local user for the Firebox® X Edge e-Series, you select the Administrative Access level for that user. You select access control for the external network and the Branch Office VPN tunnel, and time limits on this access. You also can apply a WebBlocker profile to the user account and configure the user's MUVPN restrictions.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

3 Below **Local User Accounts**, click **Add**.
The New User page appears. It shows the Settings tab.



4 In the **Account Name** field, type a name for the account. The user types this name when authenticating.
The account name is case sensitive.

5 In the **Full Name** field, type the first and last name of the user.
This is for your information only. A user does not use this name during authentication.

6 In the **Description** field, type a description for the user.
This is for your information only. A user does not use this description during authentication.

7 In the **Password** field, type a password with a minimum of eight characters.
Mix eight letters, numbers, and symbols. Do not use a word you can find in a dictionary. For increased security use a minimum of one special symbol, a number, and a mixture of uppercase and lowercase letters.

8 Type the password again in the **Confirm Password** field.

9 In the **Administrative Access** drop-down list, set the level to which your user can see and change the Firebox X Edge configuration properties: None, Read-Only, or Full.

Note

If you have Read-Only or Full access, the Firebox X Edge configuration pages appear when you authenticate to the Edge. If you have an Administrative access of None, the Login Status dialog box appears when you authenticate to the Edge. If you have Read-Only or Full access, you can click on the Authenticate User link at the bottom of the navigation pane on the left to open the Login Status dialog box.

For more information, see "Creating a read-only administrative account," on page 114.

10 In the **Session maximum time-out** field, set the maximum length of time the computer can send traffic to the external network or across a Branch Office VPN tunnel. If this field is set to zero (0) minutes, there is no session time-out and the user can stay connected for any length of time.

11 In the **Session idle time-out** field, set the length of time the computer can stay authenticated when it is idle (not passing any traffic to the external network or across the Branch Office VPN or to the Firebox X Edge itself). A setting of zero (0) minutes means there is no idle time-out.

12 If you want this user to have Internet access, select the **Allow access to the External Network** check box.
You must require user authentication for this setting to have an effect.

13 If you want this user to have access to computers on the other side of a Branch Office VPN tunnel, select the **Allow access to VPN** check box.
You must require user authentication for this setting to have an effect.

14 Click **Submit**.

Creating a read-only administrative account

You can create a local user account with access to see Firebox X Edge e-Series configuration pages. When you log in as a read-only administrator, you cannot:

- Click the **Reboot** button on the System Status page.
- Change the configuration mode on the External page.
- Click the **Reset Event Log** and **Sync Time with Browser Now** buttons on the Logging page.
- Click the **Synchronize Now** button on the System Time page.
- Click the **Regenerate IPSec Keys** button on the VPN page.
- Change the configuration mode on the Managed VPN page.
- Launch configuration wizards from the Wizard page.

If you try to do these things, you get a message that tells you that you have read-only access and cannot change the configuration file.

To create a read-only user account, edit the user account. Use the **Administrative Access** drop-down list to select **Read Only**.

Setting a WebBlocker profile for a user

A WebBlocker profile is a unique set of restrictions you can apply to users on your network. To apply a WebBlocker profile to a user's account, click the **WebBlocker** tab and select a profile from the drop-

down list. You must first create WebBlocker profiles in the **WebBlocker > Profiles** area of the Firebox X Edge configuration pages. For more information on WebBlocker profiles, see "Creating WebBlocker Profiles" on page 123.

Enabling MUVPN for a user

To enable MUVPN for a new user, see "Connecting and Disconnecting the MUVPN Client" on page 156.

The Administrator account

The Firebox X Edge e-Series has a built-in administrator account that cannot be deleted. You can change some of the administrator account settings. On the Firebox Users page, click the icon in the **Edit** column of the administrator account.

For descriptions of the fields, see "Using Local Firebox Authentication" on page 113.

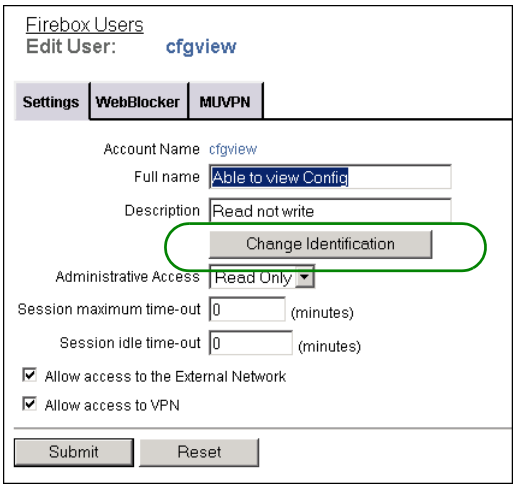
Make sure you keep the administrator name and password in a safe location. You must have this information to see the configuration pages. If the system administrator name and password are not known, you must reset the Firebox X Edge to the factory default settings. For more information, see "Factory Default Settings" on page 33.

We recommend that you change the administrator passphrase at regular intervals. Use a passphrase of at least eight letters, numbers, and symbols. Do not use a word from an English or other dictionary. Use one or more symbols, a number, and a mixture of uppercase and lowercase letters for increased security.

Changing a user account name or password

You can change an account name or account password. If you change the account name, you must give the account password.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
   The default URL is: https://192.168.111.1.
2. From the navigation bar, select **Firebox Users**.
   The Firebox Users page appears.
3. Below **Local User Accounts**, click **Edit** for the account to change the password for.
   The Edit User page appears with the Settings tab visible.
4. Click **Change Identification**.
5. Type the old password and a new password. Confirm the new password.
6. Click **Submit**.



Using LDAP/Active Directory Authentication

If you use LDAP authentication, you do not have to keep a separate user database on the Firebox® X Edge. You can configure the Edge to forward user authentication requests to a generic LDAP or Active Directory server. You can use LDAP authentication and local Firebox authentication at the same time.

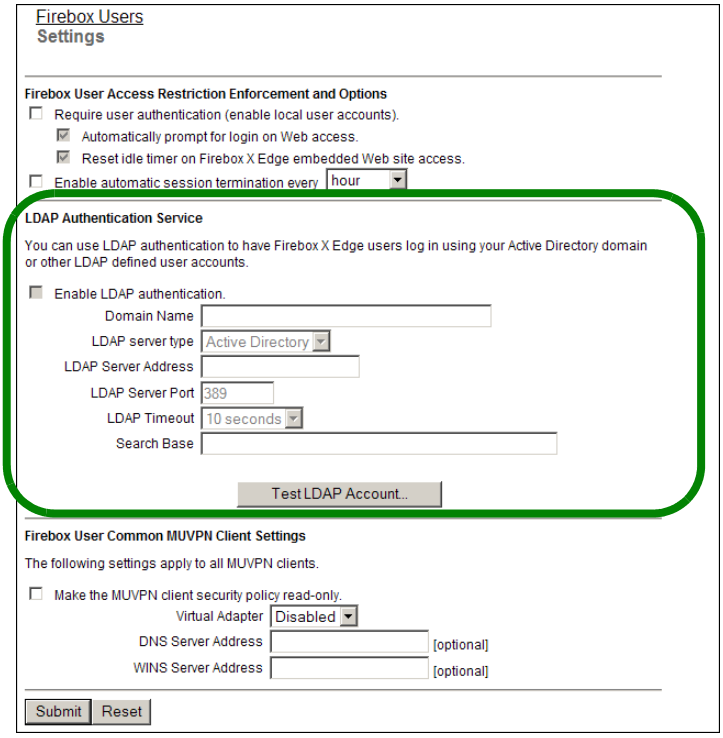
With LDAP authentication, user privileges are controlled on a group basis. You can add the names of your existing LDAP or Active Directory user groups to the Firebox X Edge configuration and assign privileges and a WebBlocker profile. When users authenticate to the Edge, they prepend their LDAP domain name to their user name in the authentication dialog box (domain\user name). If you use an Active Directory authentication server, users can also authenticate using their fully qualified domain name (username@mycompany.com).

Configuring the LDAP/Active Directory authentication service

When you enable LDAP authentication, you define one authentication server and its properties. To enable LDAP authentication:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Firebox Users > Settings**.
The Firebox Users Settings page appears.


Firebox Users
Settings
Firebox User Access Restriction Enforcement and Options
Require user authentication (enable local user accounts).
Automatically prompt for login on Web access.
Reset idle timer on Firebox X Edge embedded Web site access.
Enable automatic session termination every
hour
LDAP Authentication Service
You can use LDAP authentication to have Firebox X Edge users log in using your Active Directory domain or other LDAP defined user accounts.
Enable LDAP authentication.
Domain Name
LDAP server type
Active Directory
LDAP Server Address
LDAP Server Port
389
LDAP Timeout
10 seconds
Search Base
Test LDAP Account...
Firebox User Common MUVPN Client Settings
The following settings apply to all MUVPN clients.
Make the MUVPN client security policy read-only.
Virtual Adapter
Disabled
DNS Server Address
[optional]
WINS Server Address
[optional]
Submit
Reset

3 Select the **Enable LDAP authentication** check box.
If user authentication is not enabled in the top section of this configuration page, the LDAP Authentication Service section is not active.

4 In the **Domain Name** text box, type the name of the LDAP domain. Do not include the top-level domain.
The domain (or host) name is the part of your company's URL that ends with .com, .net, .org, .biz, .gov, or .edu. For example, if your company URL is mycompany.com, type mycompany in the Domain Name text box.

5 From the **LDAP server type** drop-down list, select the type of LDAP implementation you use in your organization: **Active Directory** or **Generic LDAP**.

6 In **LDAP Server Address** text box, type the IP address of the LDAP server the Firebox X Edge will use for authentication requests.
The LDAP server can be located on any Edge interface or available through a VPN tunnel.

7 In the **LDAP Server Port** text box, type the port number the Firebox X Edge will use for connections to the LDAP server.
The default LDAP server port number is 389. Usually you do not have to change this number.

8 Use the **LDAP Timeout** drop-down list, select the number of seconds to use as a time-out for any LDAP operation.

9 In the **Search Base** text box, type the base in the LDAP directory to start the search for user account entries. This must be a legitimate LDAP DN (Distinguished Name).
A Distinguished Name is a name that uniquely identifies an entry in an LDAP directory. A DN includes as many qualifiers as it must to find an entry in the directory. For example, a DN can look like this:
OU=user accounts,DC=mycompany,DC=com

10 If you select Generic LDAP as the LDAP server type, you must enter a **Login Attribute Name** and **Group Attribute Name** in the appropriate text boxes. These text boxes do not appear if you select Active Directory as the LDAP server type.
The **Login Attribute Name** is the name of the login name attribute of user entries in the LDAP directory.

The **Group Attribute Name** is the name of the group membership attribute of user entries in the LDAP directory.

11 Click **Submit**.

Using the LDAP authentication test feature

After the Firebox X Edge e-Series is configured to use LDAP authentication, you can use the LDAP authentication test feature to make sure the Edge can connect to the LDAP server. You can use the test for a specified user account to make sure that the Edge can successfully send and receive authentication requests for that user.

To use the test feature, click **LDAP Authentication Test** and type the name and password of an LDAP user account. The user name must be typed in the domain\user name format, such as mycompany\admin.

The results of the authentication attempt are shown on the screen. If the authentication is successful, the User Permissions section shows the access rights for this user account.

Configuring groups for LDAP authentication

Account privileges for users that authenticate to an LDAP server are set based on group membership. The group that the user is in sets all privileges for that user except MUVPN. MUVPN privileges must be set at the user level.

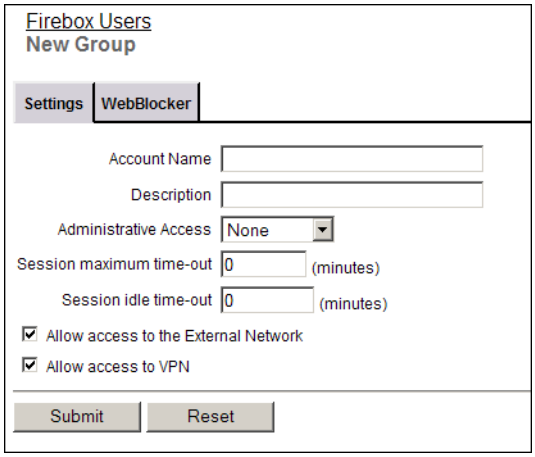
The name you give to a group on the Firebox X Edge must match the name of the group assigned to user entries in the LDAP directory. On the Edge, there is a built-in default group. The settings of the default group apply to any LDAP user that does not belong to any group configured on the Edge. You can change the properties of the default group, but you cannot delete the default group.

If a user belongs to more than one group, the privileges for that user are set to the least restrictive settings of all groups to which the user belongs. In WebBlocker, the least restrictive profile is the profile with the lowest number of blocked categories. For a more general example, a group “admins” allows administrative access, but the the group “powerusers” gives read-only access, and the group “everyone” gives no administrative access. A user that belongs to all three groups gets administrative access because it is the least restrictive setting of the three.

Adding a group

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Firebox Users > New Group**.
The Firebox Users New Group page appears.



3 In the **Account Name** text box, type the name of the new group. This name must match the name of a group in the LDAP directory.
This name must contain only letters, numbers, and the underscore (_)or dash (-) characters. Spaces are not permitted.

4 In the **Description** text box, you can enter a description of the group. This field is optional.

5 From the **Administrative Access** drop-down list, select the level of Firebox X Edge administrative access to assign to the group. You can select:
None - The members of the group have no access to Firebox X Edge administration functions.
Read-only - The members of this group can see, but not change, Firebox X Edge configuration and status.
Full - The members of this group have full Firebox X Edge administrative privileges.

6 Use the **Session maximum time-out** text box to set the number of minutes a user session started by a member of this group is allowed to stay active. When this limit occurs, the Firebox X Edge will close the session.

7 Use the **Session idle time-out** text box to set the number of minutes a user session started by a member of this group can stay idle before it is automatically closed by the Firebox X Edge.

8 Select the **Allow access to the External Network** check box to allow the members of this group to access the external network through the Firebox X Edge.

9 Select the **Allow access to VPN** check box to allow the members of this group to access VPN tunnels using the Firebox X Edge.

10 Click **Submit**.

Setting a WebBlocker profile for a user

A WebBlocker profile is a unique set of restrictions you can apply to users on your network to control access to external Web sites. To apply a WebBlocker profile to the group, click the **WebBlocker** tab on the Firebox Users New Group page and select a profile from the drop-down list. You must first create WebBlocker profiles in the **WebBlocker > Profiles** area of the Firebox X Edge configuration pages. If no profile is assigned, the users in this group have full access to all web sites. For more information on WebBlocker profiles, see “Creating WebBlocker Profiles” on page 123.

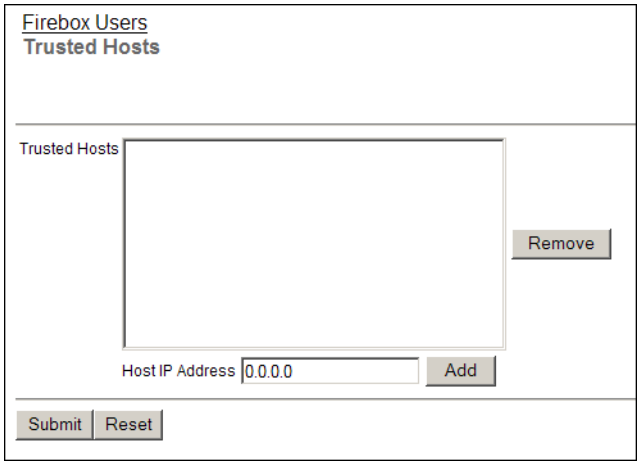
LDAP Authentication and MUVPN

Because MUVPN settings cannot be assigned at the group level, you must create a local Firebox user account for the user and add MUVPN settings for the user on the MUVPN. See "Using Local Firebox Authentication" on page 113 for more information.

Allowing Internal Hosts to Bypass User Authentication

You can make a list of internal hosts that bypass user authentication settings. If a host is on this list, a user at that host does not have to authenticate to get access to the Internet. No WebBlocker rules apply to web traffic originating from hosts on this list.

1 From the navigation bar, select **Firebox Users > Trusted Hosts**.
The Firebox Users Trusted Hosts page appears.



2 In the **Host IP Address** text box, type the IP address of the computer on your trusted or optional network to allow to browse the Internet without authentication restrictions.

3 Click **Add**.
Repeat step 2 for other trusted computers.

4 Click **Submit**.

To remove a computer from the list, select the address and click **Remove**.

CHAPTER 11 Configuring WebBlocker

WebBlocker is an option for the Firebox® X Edge e-Series that gives you control of the web sites that are available to your users. Some companies restrict access to some web sites to increase employee productivity. Other companies restrict access to offensive web sites.

Note

You must purchase the WebBlocker upgrade to use this feature.

How WebBlocker Works

WebBlocker uses a database of web site addresses controlled by SurfControl®, a web filter company.

When a user on your network tries to connect to a web site, the Firebox® X Edge e-Series examines the WebBlocker database. If the web site is not in the database or is not blocked, the page opens. If the web site is in the WebBlocker database and is blocked, a notification appears and the web site is not displayed.

Configuring Global WebBlocker Settings

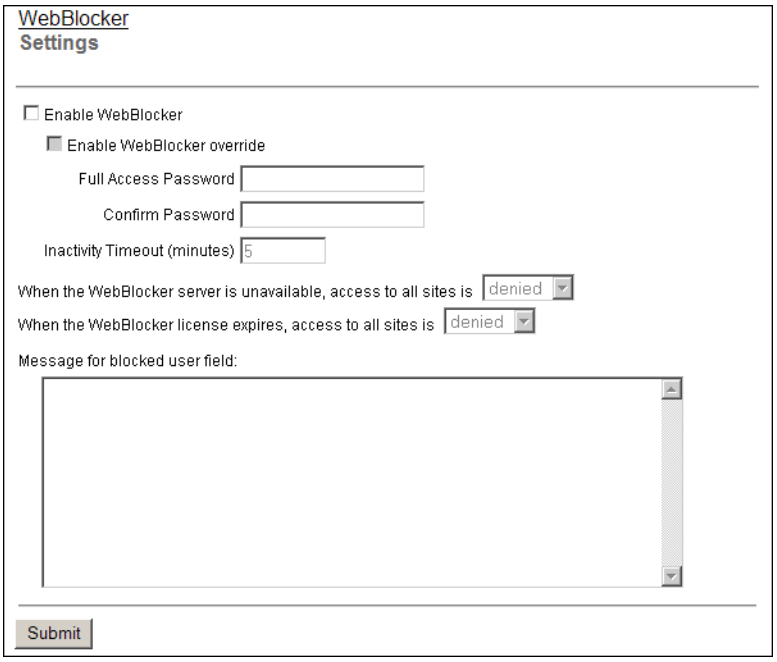
The first WebBlocker page in the Firebox® X Edge e-Series configuration pages is the WebBlocker Settings page. Use this page to:

- Activate WebBlocker
- Set the full access password
- Set the inactivity time-out
- Set an action if the Edge cannot connect to the WebBlocker server
- Set an action if the WebBlocker license expires
- Add a custom message for users to see when WebBlocker denies access to a web site

To configure WebBlocker:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **WebBlocker > Settings.**
The WebBlocker Settings page appears.



3 Select the **Enable WebBlocker** check box to turn on the WebBlocker feature.

4 If you want to allow users to bypass WebBlocker if they know the full access password, select the **Enable WebBlocker override** check box. Type a password in the **Full Access Password** field, then type the same password again in the **Confirm Password** field.
The full access password gives access to all web sites until the inactivity timeout is reached or until an authenticated user logs out.

5 Type a number, in minutes, in the **Inactivity Timeout** field.
The Inactivity Timeout shows the length of time the Full Access Password is active if no web browsing is done. If a user types the Full Access Password and no HTTP traffic is done from that user's computer for the length of time set in the Inactivity Timeout, WebBlocker rules start again. The value can be from 1 to 1440 minutes.

6 Use the **When the WebBlocker server is unavailable, access to all sites is** drop-down list to select if the Firebox X Edge is to allow or deny all traffic when it cannot connect to the WebBlocker server.
If you allow web traffic when the WebBlocker server is unavailable, each user who sends a web request must wait 45 seconds for the Firebox X Edge to try to connect to the WebBlocker server and time-out. After 45 seconds, the Edge allows access to the web site. When the Edge can connect to the WebBlocker server again, it will automatically start to apply WebBlocker rules again.

7 Use the **When the WebBlocker license expires, access to all sites is** drop-down list to select if the Firebox X Edge is to allow or deny all web traffic if the WebBlocker subscription expires.
If the WebBlocker subscription is renewed, the Firebox X Edge keeps the previous configuration and applies WebBlocker rules again.

8 Add a custom message for users to see when they try to access a web page that is blocked by WebBlocker. This message appears with the usual WebBlocker message.
For example, you can enter a message "This web site does not comply with our Internal Use Policy." If a user tries to access a web site that is blocked by WebBlocker, the user's browser shows:

```
Request for URL http://www.some-denied-site.com/denied by WebBlocker:
blocked for
```

```
Adult/Sexually Explicit.
This web site does not comply with our Internal Use Policy.
```

9 Click **Submit**.

Creating WebBlocker Profiles

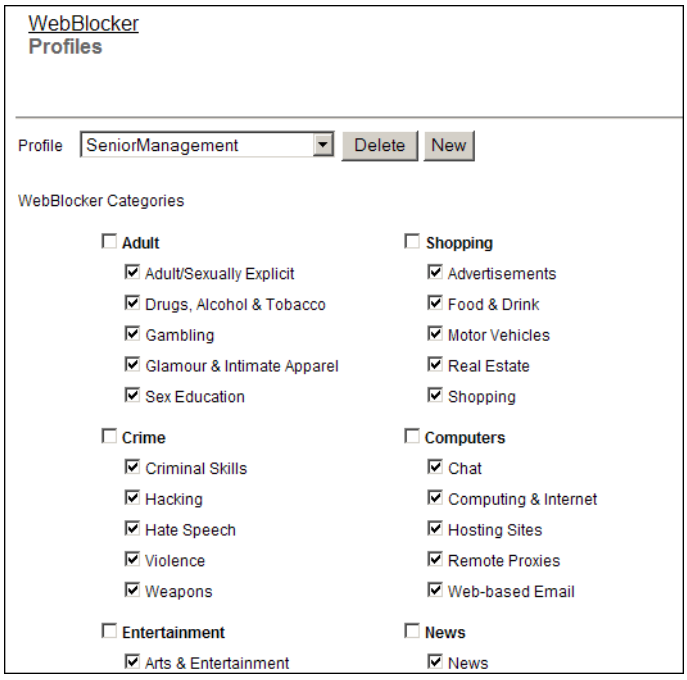
A WebBlocker profile is a set of restrictions you apply to users or groups of users on your network. You can create different profiles, with different groups of restrictions. For example, you can create a profile for new employees with more restrictions than for other employees. It is not necessary to create WebBlocker profiles if you use one set of WebBlocker rules for all of your users.

After you create profiles, you can apply them when you set up Firebox® X Edge user accounts. This procedure appears in Chapter 10, "Managing Users and Groups."

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, click **WebBlocker > Profiles**.
The Profiles page appears.

3 Click **New**.
The New Profile page appears.



4 In the **Profile Name** field, type a familiar name.
Use this name to identify the profile during configuration. For example, give the name "90day" to a group of employees at your company that work for less than 90 days.

5 In **WebBlocker Categories** select the categories of web sites to block by clicking the check box adjacent to the category name.
For more information on categories, see the next section. If you select the check box adjacent to a category group, it automatically selects all of the categories in that group. If you clear the check box adjacent to a category group, all of the categories in that group are deselected.

6 Click **Submit**.

To remove a profile, from the WebBlocker Profiles page, select the profile from the **Profile** drop-down list. Click **Delete**.

Note

If you do not use user authentication, the default WebBlocker profile is applied to all users. For more information about user authentication, see Chapter 10, "Managing Users and Groups".

WebBlocker Categories

The WebBlocker database contains nine groups of categories with 40 individual categories. A web site is added to a category when the contents of the web site meet the correct criteria. Web sites that give opinion or educational material about the subject matter of the category are not included. For example, the drugs/drug culture category denies sites that tell how to use marijuana. They do not deny sites with information about the historical use of marijuana.

Category	Description of Content
Adult/ Sexually Explicit	• Sexually oriented or erotic full or partial nudity • Depictions or images of sexual acts, including inanimate objects used in a sexual manner • Erotic stories and textual descriptions of sex acts • Sexually exploitive or sexually violent text or graphic • Bondage, fetishes, genital piercing • Adult products including sex toys, CD-ROMs, and videos • Adult services including videoconferencing, escort services, and strip clubs • Explicit cartoons and animation • Child pornograpy/pedophilia • Online groups, including newsgroups and forums that are sexually explicit in nature • Naturist sites that feature nudity • Erotic or fetish photography that depicts nudity
Advertise-ments	• Banner Ad servers • Pop-up advertisements • Adware
Arts & Entertain-ment	• Television, movies, music, and video programming guides • Comics, jokes, movie, video, or sound clips • Performing arts (theater, vaudeville, opera, symphonies, etc.) • Online magazines and reviews on the entertainment industry • Dance companies, studios, and training • Broadcasting firms and technologies (satellite, cable, etc.) • Book reviews and promotions, variety magazines, and poetry • Jokes, comics, comic books, comedians, or any site designed to be funny or satirical • Online museums, galleries, artist sites (including sculpture, photography, etc.) • Celebrity fan sites • Horoscopes • Online greeting cards • Amusement/theme parks
Chat	• Web-based chat • Instant Message servers

Category	Description of Content
Computing and Internet	• Reviews, information, computer buyer's guides, computer parts and accessories, and software • Computer/software/Internet companies, industry news, and magazines • Pay-to-surf sites • Downloadable (non-streaming) movie, video, or sound clips • Downloadable mobile phone/PDA software, including themes, graphics, and ringtones • Freeware and shareware sites • Personal storage and backup • Clip art, fonts, and animated GIF pages Note: Does not include update sites for operating systems, anti-virus agents, or other business-critical programs.
Criminal Skills	• Advocating, instructing, or giving advice on performing illegal acts • Tips on evading law enforcement • Lock-picking and burglary techniques • Phishing • Phone service theft advice • Plagiarism and cheating, including the sale of research papers
Drugs, Alcohol, & Tobacco	• Recipes, instructions, or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage • Glamorizing, encouraging, or instructing in the use of or masking the use of alcohol, tobacco, illegal drugs, and other substances that are illegal to minors • Alcohol and tobacco promotional web sites • Information on "legal highs": glue sniffing, misuse of prescription drugs, and abuse of other legal substances • Distributing alcohol, illegal drugs, or tobacco free or for a charge • Displaying, selling, or detailing the use of drug paraphernalia Note: SurfControl does not include sites that discuss medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. SurfControl also does not include sites sponsored by a public or private agency that provide educational information on drug use.
Education	• Educational institutions, including pre-, elementary, secondary, and high schools; universities • Educational sites: pre-, elementary, secondary, and high schools; univerisities • Distance education, trade schools, and online courses • Online teacher resources (lesson plans, etc.)
Finance & Investment	• Stock quotes, stock tickers, and fund rates • Online stock or equity trading • Online banking and bill-pay services • Investing advice or contacts for trading securities • Money management/investment services or firms • General finances and companies that advise thereof • Accountants, actuaries, banks, mortgages, and general insurance companies

Category	Description of Content
Food & Drink	• Recipes, cooking instruction and tips, food products, and wine advisors • Restaurants, cafes, eateries, pubs, and bars • Food/drink magazines and reviews
Gambling	• Online gambling or lottery web sites that invite the use of real money • Information or advice for placing wagers, participating in lotteries, gambling real money, or running numbers • Virtual casinos and offshore gambling ventures • Sports picks and betting pools • Virtual sports and fantasy leagues that offer large rewards or request significant wagers Note: Casino/hotel/resort sites that do not feature online gambling or provide gaming tips are categorized under Travel.
Games	• Game playing or downloading; game hosting or contest hosting • Tips and advice on games or obtaining cheat codes (“cheatz”) • Journals and magazines dedicated to online game playing
Glamour & Intimate Apparel	• Lingerie, negligee or swimwear modeling • Model fan pages; fitness models/sports celebrities • Fashion or glamour magazines online • Beauty and cosmetics • Modeling information and agencies
Govern-ment & Politics	• Government services such as taxation, armed forces, customs bureaus, and emergency services • Local government sites • Political debate, canvassing, election information, and results • Local, national, and international political sites • Conspiracy theorist and alternative govenment views that are not hate based
Hacking	• Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, or gaining access to other computers and/or computerized communication systems • Sites that provide instruction or work-arounds for filtering software • Cracked software and information sites; “warez” • Pirated software and multimedia download sites • Computer crime • Sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, an end user or organization • Sites that distribute malicious executables or viruses • 3rd-party monitoring and other unsolicited commercial software

Category	Description of Content
Hate Speech	• Advocating or inciting degradation of or attacks on specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation • Promoting a political or social agenda that is supremacist in nature or exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation • Holocaust revisionist/denial sites • Coercion or recruitment for membership in a gang* or cult** • Militancy, extremist • Flagrantly insensitive or offensive material, including lack of recognition or respect for opposing opinions or beliefs Note: SurfControl does not include news, historical, or press incidents that may include the above criteria in this category (except in graphic examples). *A gang is defined as: a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group. **A cult is defined as: a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic, the will of the individual is subordinate to the group, and the group is outside society.
Health & Medicine	• General health such as fitness and well-being • Alternative and complementary therapies, including yoga, chiropractic, and cranio-sacral • Medical information and reference about ailments, conditions, and drugs • Medical procedures, including elective and cosmetic surgery • Hospital, medical insurance • Dentistry, optometry, and other medical-related sites • General psychiatry and mental well-being sites • Promoting self-healing of physical and mental abuses, ailments, and addictions • Psychology, self-help books, and organizations
Hobbies & Recreation	• Recreational pastimes such as collecting, gardening, or kit airplanes • Outdoor recreational activities such as hiking, camping, rock climbing • Tips or trends focused on a specific art, craft, or technique • Online publications on a specific pastime or recreational activity • Online clubs, associations or forums dedicated to a hobby • Traditional (board, card, etc.) games and their enthusiasts • Animal/pet related sites, including breed-special sites, training, shows, and humane societies • Beauty and cosmetics

Category	Description of Content
Hosting Sites	• Web sites that host business and individual web pages (i.e. GeoCities, earthlink.net, AOL)
Job Search & Career Develop-ment	• Employment agencies, contractors, job listings, career information • Career searches, career networking groups
Kids' Sites	• Child-centered sites and sites published by children
Lifestyle & Culture	• Homelife and family related topics, including weddings, births, and funerals • Parenting tips and family planning • Gay/lesbian/bisexual (non-pornographic) sites • Foreign cultures, socio-cultural information • Tattoo, piercing parlors (non-explicit)
Motor Vehicles	• Car reviews, vehicle purchasing or sales tips, parts catalogs • Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks, and RVs • Journals and magazines on vehicle modification, repair, and customization • Online automotive enthusiast clubs
News	• Newspapers online • Headline news sites, newswire services, and personalized news services • Weather sites
Personals & Dating	• Singles listings, matchmaking and dating services • Advice for dating or relationships; romance tips and suggestions
Photo Searches	• Sites that provide resources for photo and image searches • Online photo albums/digital photo exchange • Image hosting
Real Estate	• Home, apartment, and land listings • Rental or relocation services • Tips on buying or selling a home • Real estate agents • Home improvement
Reference	• Personal, professional, or educational reference • Online dictionaries, maps, and language translation sites • Census, almanacs, and library catalogs • Topic-specific search engines
Religion	• Churches, synagogues, and other houses of worship • Any faith or religious beliefs, including non-traditional religions such as Wicca and witchcraft
Remote Proxies	• Remote proxies or anonymous surfing • Web-based translation sites that circumvent filtering • Peer-to-peer sharing
Search Engines	• General search engines (Yahoo, AltaVista, Google)

Category	Description of Content
Sex Education	• Pictures or text advocating the proper use of contraceptives, including condom use, the correct way to wear a condom, and how to put a condom in place • Sites related to discussion about the use of birth control pills, IUDs, and other types of contraceptives • Discussion sites on how to talk to your partner about diseases, pregnancy, and respecting boundaries Note: Not included in this category are commercial sites that sell sexual paraphernalia. These sites are filtered through the Adult category.
Shopping	• Department stores, retail stores, company catalogs, and other sites that allow online consumer shopping • Online auctions • Online downloadable product warehouses; specialty items for sale • Freebies or merchandise giveaways
Sports	• Team or conference web sites • National, international, college, or professional scores and schedules • Sports-related online magazines or newsletters • Fantasy sports and virtual sports leagues that are free or low-cost
Streaming Media	• Streaming media files or events (any live or archived audio or video file) • Internet TV and radio • Personal (non-explicit) Webcam sites • Telephony sites that allow user to make calls via the Internet • VoIP services
Travel	• Airlines and flight booking agencies • Accommodation information • Travel package listings • City guides and tourist information • Car rentals

Category	Description of Content
Violence	• Portraying, describing, or advocating physical assault against humans, animals, or institutions • Depictions of torture, mutilation, gore, or horrific death • Advocating, encouraging, or depicting self-endangerment or suicide, including the use of eating disorders or addictions • Instructions, recipes, or kits for making bombs and other harmful or destructive devices • Sites promoting terrorism • Excessively violent sports or games (including video and online games) • Offensive or violent language, including through jokes, comics, or satire • Excessive use of profanity or obscene gesticulation Note: We do not block news, historical, or press incidents that may include the above criteria (except in graphic examples).
Weapons	• Online purchasing or ordering information, including lists of prices and dealer locations • Any page or site predominantly containing, or providing links to, content related ot the sale of guns, weapons, ammunition, or poisonous substances • Displaying or detailing the use of guns, weapons, ammunition or poisonous substances • Clubs that offer training on machine guns, automatic guns, other assault weapons, and/or sniper training Note: Weapons are defined as something (as a club, knife, or gun) used to injure, defeat, or destroy.
Web-based E-mail	• Web-based e-mail accounts • Messaging sites (SMS, etc)
Usenet/ Forums	• Opinion or discussion forums • Weblogs (blog) sites

For information on how to see if a web site is included in the SurfControl database, read the “How can I see a list of blocked sites?” topic in this FAQ:

https://www.watchguard.com/support/AdvancedFaqs/web_main.asp

You must log in to your LiveSecurity account to see this FAQ.

Allowing Certain Sites to Bypass WebBlocker

WebBlocker can deny a web site that is necessary for your work. You can override WebBlocker using the Allowed Sites feature.

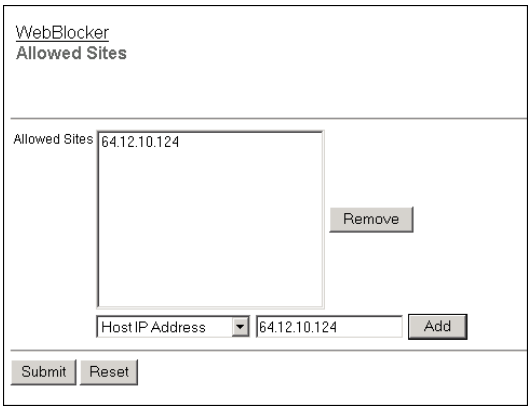
For example, employees in your company frequently use web sites that contain medical information. Some of these web sites are forbidden by WebBlocker because they fall into the sex education category. To override WebBlocker, you add the web site's IP address or its domain name to the Allowed Sites record.

Note

This WebBlocker feature only applies to web sites on the Internet. You cannot use WebBlocker to block your users from web sites behind the Firebox®.

1 From the navigation bar, select **WebBlocker > Allowed Sites.**
The WebBlocker Allowed Sites page appears.

2 From the drop-down list, select host IP address or domain name.



3 Type the host IP address or domain name of the web site to allow.
Repeat step 3 for each additional host or domain name that you wish to add to the Allowed Sites list.
The domain (or host) name is the part of a URL that ends with .com, .net, .org, .biz, .gov, or .edu. Domain names may also end in a country code, such as .de (Germany) or .jp (Japan).
To add a domain name, type the URL pattern without the leading "http://". For example, to allow access to the Google web site, select to add a domain name and enter "google.com".
If the site has a subdomain that resolves to a different IP address, you must enter that subdomain to allow it. For example, if "www.site.com" and "site.com" are on different servers, you must add both entries.

4 Click **Add**.
The site is added to the Allowed Sites list.

5 Click **Submit**.

To remove an item from the Allowed Sites list, select the address and click **Remove**, then click **Submit**.

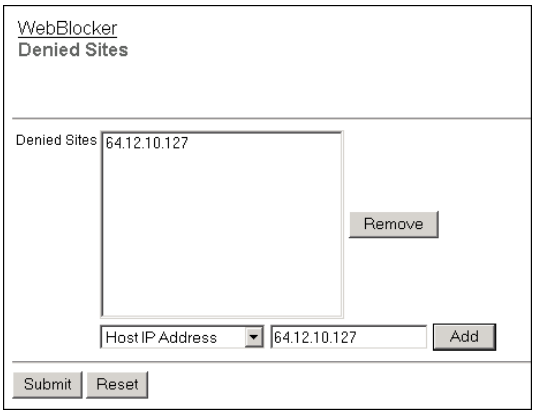
Blocking Additional Web Sites

You can block some web sites that WebBlocker allows. For example, you can receive a LiveSecurity® Service alert that tells you that a frequently used web site is dangerous. Use the Denied Sites feature to add

the web site's IP address or domain name to WebBlocker to make sure your employees cannot not look at this web site.

1 From the navigation bar, select **WebBlocker > Denied Sites**.
The WebBlocker Denied Sites page appears.

2 From the drop-down list, select host IP address or domain name.



3 Type the host IP address or domain name of the denied web site.
Repeat step 3 for each additional host, IP address, or domain name you wish to add to the Denied Sites list.
The domain (or host) name is the part of a URL that ends with .com, .net, .org, .biz, .gov, or .edu. Domain names also can end in a country code, such as .de (Germany) or .jp (Japan).
To add a domain name, type the URL pattern without the leading "http://". For example, to allow access to the Playboy web site, select to add a domain name and enter "playboy.com". If the site has a subdomain that resolves to a different IP address, you must enter that subdomain to deny it. For example, if "www.site.com" and "site.com" are on different servers, you must add both entries.

4 Click **Add**.
The site is added to the Denied Sites list.

5 Click **Submit**.

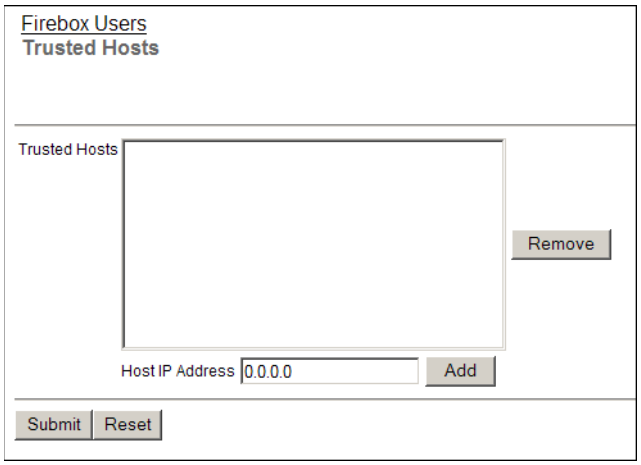
To remove an item from the Denied Sites list, select the address and click **Remove** and then click **Submit**.

Bypassing WebBlocker

You can make a list of internal hosts that bypass WebBlocker. The internal hosts that you put on this list also bypass any user authentication settings. If a user is on this list, that user does not have to authenti-

cate to get access to the Internet. No WebBlocker rules apply to the users on this list. For more information about user authentication, see “Managing Users and Groups” on page 107.

1 From the navigation bar, select **Firebox Users > Trusted Hosts**.
The Firebox Users Trusted Hosts page appears.



2 In the **Host IP Address** text box, type the IP address of the computer on your trusted or optional network to allow to browse the Internet without authentication restrictions.

3 Click **Add**.
Repeat step 2 for other trusted computers.

4 Click **Submit**.
To remove a computer from the list, select the address and click Remove.

CHAPTER 12

Configuring Virtual Private Networks

A VPN (Virtual Private Network) creates secure connections between computers or networks in different locations. This connection is known as a tunnel. The networks and hosts on a VPN tunnel can be corporate headquarters, branch offices, remote users, or telecommuters. When a VPN tunnel is created, the two tunnel endpoints are authenticated. Data in the tunnel is encrypted. Only the sender and the recipient of the message can read it.

About This Chapter

This chapter starts with a section that tells you the basic requirements for your Firebox® X Edge e-Series to create a VPN. Start with "What You Need to Create a VPN" on page 135.

The subsequent section tells you how to configure the Firebox X Edge to be the endpoint of a VPN tunnel created and managed by a WatchGuard® Firebox X Core or Peak Management Server. This procedure is different for different versions of WatchGuard System Manager appliance software installed on the Firebox X Core or Peak. This section also gives procedures for VPN tunnels managed by VPN Manager (available with earlier versions of Watchguard management software).

Information about how to configure a Manual VPN to connect to another VPN device also is included in this chapter. Use this section to create VPN tunnels to any other IPSec VPN endpoint.

The last part of this chapter includes frequently asked questions, information on how to keep the VPN tunnel operating correctly, and instructions on how to see VPN tunnel statistics. These last sections can help you troubleshoot problems with VPN.

For more information on VPN tunnels, see the FAQ information available at

https://www.watchguard.com/support/kb/

What You Need to Create a VPN

Before you configure your WatchGuard® Firebox® X Edge VPN network, read these requirements:

- You must have two Firebox X Edge devices or one Firebox X Edge and a second device that uses IPSec standards. Examples of these devices are a Firebox III, Firebox X Core, Firebox X Peak, or a Firebox SOHO 6. You must enable the VPN option on the other device if it is not already active.

- You must have an Internet connection.
- The ISP for each VPN device must let IPSec go across their networks.

Some ISPs do not let you create VPN tunnels on their networks unless you upgrade your Internet service to a level that supports VPN tunnels. Speak with the ISP to make sure they let you use these ports and protocols:

  - UDP Port 500 (Internet Key Exchange or IKE)
  - UDP Port 4500 (NAT traversal)
  - IP Protocol 50 (Encapsulating Security Payload or ESP)

- If the other side of the VPN tunnel is a WatchGuard Firebox X and each Firebox is under WatchGuard System Manager management, you can use the Managed VPN option. Managed VPN is easier to configure than Manual VPN. You must get information from the administrator of the Firebox X on the other side of the VPN to use this option.
- You must know if the IP address assigned to your Firebox X Edge external interface is static or dynamic. To learn about IP addresses, see Chapter 2, "Installing the Firebox X Edge e-Series."
- Your Firebox X Edge e-Series model tells you the number of VPN tunnels that you can create on your Edge. You can purchase a model upgrade for your Edge to make more VPN tunnels, as described in "Enabling the Model Upgrade Option" on page 44.
- If you connect two Microsoft Windows NT networks, they must be in the same Microsoft Windows domain, or they must be trusted domains. This is a Microsoft Networking problem, and not a limit of the Firebox X Edge e-Series.
- If you want to use the DNS and WINS servers from the network on the other side of the VPN tunnel, you must know the IP addresses of these servers.

The Firebox X Edge can give WINS and DNS IP addresses to the computers on its trusted network if those computers get their IP addresses from the Edge using DHCP. If you want to give the computers the IP addresses of WINS and DNS servers on the other side of the VPN, you can type those addresses into the DHCP settings in the trusted network setup. For information on how to configure the Edge to give DHCP addresses, see "Using DHCP on the trusted network" on page 51.

- You must know the network address of the private (trusted) networks behind your Firebox X Edge e-Series and of the network behind the other VPN device, and their subnet masks.

Note

The private IP addresses of the computers behind your Firebox X Edge cannot be the same as the IP addresses of the computers on the other side of the VPN tunnel. If your trusted network uses the same IP addresses as the office to which it will create a VPN tunnel, then your network or the other network must change their IP address arrangement to prevent IP address conflicts.

Managed VPN

You can configure a VPN tunnel on the Firebox® X Edge e-Series with two procedures: Managed VPN and Manual VPN. For information on creating a manual VPN tunnel, see "Manual VPN: Setting Up Manual VPN Tunnels" on page 137.

The WatchGuard® Management Server (previously known as the DVCP Server) uses DVCP to keep the VPN tunnel configuration. DVCP (Dynamic VPN Configuration Protocol) is the WatchGuard protocol that you can use to create IPSec tunnels easily. We use the name Managed VPN because the Management Server manages the VPN tunnel and sends the VPN configuration to your Firebox X Edge. An Edge administrator must type only a small quantity of information into the Edge configuration pages.

You must have WatchGuard System Manager and a Firebox III, Firebox X Core, or Firebox X Peak to have a Management Server. When your Firebox X Edge gets its VPN configuration from a Management

Server, your Edge is a client of the Management Server in a client-server relationship. The Edge gets all of its VPN configuration from the Management Server.

To configure a Firebox X Edge to allow WatchGuard System Manager access for the creation of VPN tunnels, see "Setting up WatchGuard System Manager Access" on page 38.

Manual VPN: Setting Up Manual VPN Tunnels

To create a VPN tunnel manually to another Firebox® X Edge or to a Firebox III or Firebox X, or to configure a VPN tunnel to a device that is not a WatchGuard® device, you must use Manual VPN. Use this section to configure Manual VPN on the Edge.

What you need for Manual VPN

In addition to the VPN requirements at the start of this chapter, you must have this information to create a manual VPN tunnel:

- You must know if the IP address assigned to the other VPN device is static or dynamic. If the other VPN device is dynamic, your Firebox X Edge must find the other device by domain name and the other device must use Dynamic DNS.
- You must know the shared key (passphrase) for the tunnel. The same shared key must be used by the two devices.
- You must know the encryption method used for the tunnel (DES or 3DES). The two VPN devices must use the same method.
- You must know the authentication method for each end of the tunnel (MD5 or SHA1). The two VPN devices must use the same authentication method.

We recommend that you write down your Firebox X Edge configuration, and the related information for the other device. Use the Sample VPN Address Information table on the subsequent page to record this information.

Sample VPN Address Information Table

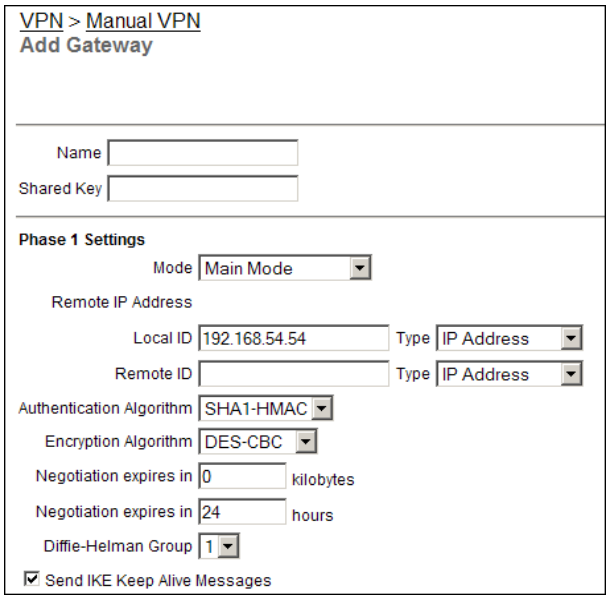
Item	Description	Assigned by
External IP Address	The IP address that identifies the IPSec-compatible device on the Internet. Example: Site A: 207.168.55.2 Site B: 68.130.44.15	ISP
Local Network Address	An address used to identify a local network. These are the IP addresses of the computers on each side that are allowed to send traffic through the VPN tunnel. We recommend that you use an address from one of the reserved ranges: 10.0.0.0/8—255.0.0.0 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0 The numbers after the slashes indicate the subnet masks. /24 means that the subnet mask for the trusted network is 255.255.255.0. For more information on entering IP addresses in slash notation, see this FAQ: https://www.watchguard.com/support/advancedfaqs/general_slash.asp You must log in to your LiveSecurity account to see the FAQ. Example: Site A: 192.168.111.0/24 Site B: 192.168.222.0/24	You
Shared Key	The shared key is a passphrase used by two IPSec-compatible devices to encrypt and decrypt the data that goes through the VPN tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly. Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, "Gu4c4mo!3" is better than "guacamole". Example: Site A: OurSharedSecret Site B: OurSharedSecret	You
Encryption Method	DES uses 56-bit encryption. 3DES uses 168-bit encryption. The 3DES encryption method is more secure, but slower. The two devices must use the same encryption method. Example: Site A: 3DES Site B: 3DES	You
Authentication	The two devices must use the same authentication method. Example: Site A: MD5 (or SHA1) Site B: MD5 (or SHA1)	You

To create Manual VPN tunnels on your Edge

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **VPN > Manual VPN**.
The Manual VPN page appears.

3 Click **Add**.
The Add Gateway page appears.



4 Type the tunnel name and shared key.
The tunnel name is for your identification only.
The shared key is a passphrase that the devices use to encrypt and decrypt the data on the VPN tunnel. The two devices must use the same passphrase, or they cannot encrypt and decrypt the data correctly.

Phase 1 settings

Internet Key Exchange (IKE) is a protocol used with VPN tunnels to manage keys automatically. IKE negotiates and changes keys. Phase 1 authenticates the two sides and creates a key management security association to protect tunnel data.

The default settings for Phase 1 are the same for all Firebox X Edge devices. Many users keep the factory default settings.

Note

Make sure that the Phase 1 configuration is the same on the two devices.

To change Phase 1 configuration:

1 Select the negotiation mode from the drop-down list.

Note

You can use Main Mode only when the two devices have static IP addresses. If one or both of the devices have external IP addresses that are dynamically assigned, you must use Aggressive Mode.

2 Enter the local ID and remote ID. Select the ID types—**IP Address** or **Domain Name**—from the drop-down lists. Make sure this configuration is the same as the configuration on the remote device.
Note that on the other device, the local ID type and remote ID type are reversed.

- If your Firebox X Edge or remote VPN device has a static external IP address, set the local ID type to **IP Address**. Type the external IP address of the Edge or device as the local ID.
- If your Firebox X Edge or remote VPN device has a dynamic external IP address, you must select **Aggressive Mode** and the device must use Dynamic DNS. For more information, see "Registering with the Dynamic DNS Service" on page 58. Set the local ID type to **Domain Name**. Enter the DynDNS domain name of the device as the local ID.

Note

If your Firebox X Edge external interface has a private IP address instead of a public IP address, then your ISP or the Internet access device connected to the Edge's external interface (modem or router) does Network Address Translation (NAT). See the instructions at the end of this section if your Edge's external interface has a private IP address.

3 Select the type of authentication from the **Authentication Algorithm** drop-down list.
The options are MD5-HMAC (128-bit authentication) or SHA1-HMAC (160-bit authentication).

4 From the **Encryption Algorithm** drop-down list, select the type of encryption.
The options are DES-CBC or 3DES-CBC.

5 Type the number of kilobytes and the number of hours until the IKE negotiation expires.
To make the negotiation never expire, enter zero (0). For example, 24 hours and zero (0) kilobytes means that the phase 1 key is negotiated every 24 hours no matter how much data has passed.

6 Select the group number from the **Diffie-Hellman Group** drop-down list. We support group 1 and group 2.
Diffie-Hellman groups securely negotiate secret keys through a public network. Group 2 is more secure than group 1, but uses more processing power and more time.

7 Select the **Send IKE Keep Alive Messages** check box to help find when the tunnel is down.
Select this check box to send short packets across the tunnel at regular intervals. This helps the two devices to see if the tunnel is up. If the Keep Alive packets get no response after three tries, the Firebox X Edge starts the tunnel again.

Note

The IKE Keep Alive feature is different from the VPN Keep Alive feature in "VPN Keep Alive," on page 142.

If your Edge is behind a device that does Network Address Translation (NAT)

The Firebox X Edge e-Series can use NAT Traversal. This means that you can make VPN tunnels if your ISP does NAT (Network Address Translation) or if the external interface of your Edge is connected to a device that does NAT. We recommend that the Firebox X Edge external interface have a public IP address. If that is not possible, use this section for more information.

Devices that do NAT frequently have some basic firewall features built into them. To make a VPN tunnel to your Firebox X Edge e-Series when the Edge is behind a device that does NAT, the NAT device must let the traffic through. These ports and protocols must be open on the NAT device:

- UDP port 500 (IKE)
- UDP port 4500 (NAT Traversal)
- IP protocol 50 (ESP)

Speak with the NAT device's manufacturer for information on opening these ports and protocols on the NAT device.

If your Firebox X Edge e-Series external interface has a private IP address, you cannot use an IP address as the local ID type in the Phase 1 settings. Because private IP addresses cannot get through the Internet, the other device cannot find the private external IP address of your Edge through the Internet.

- If the NAT device to which the Firebox X Edge is connected has a dynamic public IP address:

- First, set the device to Bridge Mode. In Bridge Mode, the Edge gets the public IP address on its external interface. Refer to the manufacturer of your NAT device for more information.
- Set up Dynamic DNS on the Firebox X Edge. For information, see "Registering with the Dynamic DNS Service" on page 58. In the Phase 1 settings of the Manual VPN, set the local ID type to **Domain Name**. Enter the DynDNS domain name as the Local ID. The remote device must identify your Edge by domain name and it must use your Edge's DynDNS domain name in its Phase 1 setup.

• If the NAT device to which the Firebox X Edge is connected has a static public IP address:
- In the Phase 1 settings of the Manual VPN, set the local ID type drop-down list to **Domain Name**. Enter the public IP address assigned to the NAT device's external interface as the local ID. The remote device must identify your Firebox X Edge by domain name, and it must use this same public IP address as the domain name in its Phase 1 setup.

Phase 2 settings

Phase 2 negotiates the data management security association for the tunnel. The tunnel uses this phase to create IPSec tunnels and put data packets together.

You can use the default Phase 2 settings to make configuration easier.

Note

Make sure that the Phase 2 configuration is the same on the two devices.

To change the Phase 2 settings:

1 Select the authentication method from the **Authentication Algorithm** drop-down list.

2 Select the encryption algorithm from the **Encryption Algorithm** drop-down list.

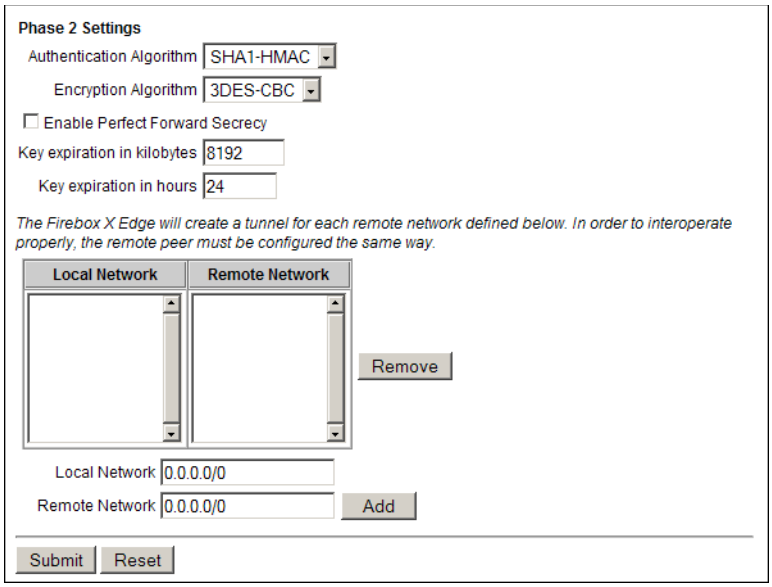
3 To use Perfect Forward Secrecy, select the **Enable Perfect Forward Secrecy** check box.
This option makes sure that each new key comes from a new Diffie-Hellman exchange. This option makes the negotiation more secure, but uses more time and computer resources.

4 Type the number of kilobytes and the number of hours until the Phase 2 key expires.
To make the key not expire, enter zero (0). For example, 24 hours and zero (0) kilobytes means that the Phase 2 key is renegotiated each 24 hours no matter how much data has passed.

5 Type the IP address of the local network and the remote networks that will send encrypted traffic across the VPN.
You must enter network addresses in "slash" notation (also known as CIDR or Classless Inter Domain Routing notation). For more information on how to enter IP addresses in slash notation, see this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.

6 Click **Add**.
Repeat step 5 if you must add additional networks.

7 Click **Submit**.

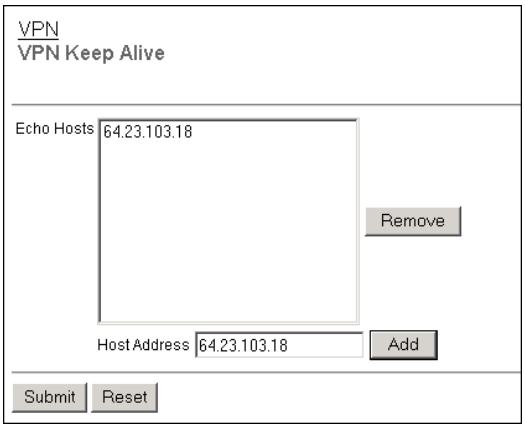


VPN Keep Alive

To keep the VPN tunnel open when there are no connections through it, you can use the IP address of a computer at the other end of the tunnel as an echo host. The Firebox® X Edge e-Series sends a ping each minute to the specified host. Use the IP address of a host that is always online and that can respond to ping messages. You can enter the trusted interface IP address of the Firebox that is at the other end of the tunnel. You also can use more than one IP address so the Edge can send a ping to more than one host through different tunnels.

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **VPN > Keep Alive**.
The VPN Keep Alive page appears.



3 Type the IP address of an echo host. Click **Add**.
Repeat step 3 to add additional echo hosts.

4 Click **Submit**.

Viewing VPN Statistics

You can monitor Firebox® X Edge e-Series VPN traffic and troubleshoot the VPN configuration with the VPN Statistics page.

To see the VPN Statistics page:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1

2 From the navigation bar, select **System Status > VPN Statistics**.
The VPN Statistics page appears.

Frequently Asked Questions

Why do I need a static external address?

To make a VPN connection, each device must know the IP address of the other device. If the address for a device is dynamic, the IP address can change. If the IP address changes, connections between the devices cannot be made unless the two devices know how to find each other.

You can use Dynamic DNS if you cannot get a static external IP address. For more information, see "Registering with the Dynamic DNS Service" on page 58.

How do I get a static external IP address?

You get the external IP address for your computer or network from your ISP or a network administrator. Many ISPs use dynamic IP addresses to make their networks easier to configure and use with many users. Most ISPs can give you a static IP address as an option.

How do I troubleshoot the connection?

If you can send a ping to the trusted interface of the remote Firebox® X Edge and the computers on the remote network, the VPN tunnel is up. The configuration of the network software or the software applications are possible causes of other problems.

Why is ping not working?

If you cannot send a ping to the local interface IP address of the remote Firebox X Edge, use these steps:

1 Ping the external address of the remote Firebox X Edge.
For example, at Site A, ping the IP address of Site B. If the ping packet does not come back, make sure the external network settings of Site B are correct. (Site B must be configured to respond to ping requests on that interface.) If the settings are correct, make sure that the computers at Site B have Internet access. If the computers at site B do not have Internet access, speak to your ISP or network administrator.

2 If you can ping the external address of each Firebox X Edge, try to ping a local address in the remote network.
From a computer at Site A, ping the internal interface IP address of the remote Firebox X Edge. If the VPN tunnel is up, the remote Edge sends the ping back. If the ping does not come back, make sure the local configuration is correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

How do I set up more than the number of allowable VPNs on my Edge?

The number of VPN tunnels that you can create on your Firebox X Edge e-Series is set by the Edge model you have. You can purchase a model upgrade for your Edge to make more VPN tunnels. You can purchase a Firebox X Edge Model Upgrade from a reseller or from the WatchGuard® web site:

http://www.watchguard.com/products/purchaseoptions.asp

CHAPTER 13 Configuring the MUVPN Client

Mobile User VPN lets remote users connect to your internal network through a secure, encrypted channel. The MUVPN client is a software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network through an unsecured network. The MUVPN client uses Internet Protocol Security (IPSec) to secure the connection.

This example shows how the MUVPN client is used:

- The MUVPN client software is installed on a remote computer.
- The remote user imports a configuration file (.wgx file) to configure the client software.
- The user connects to the Internet with the remote computer. The user starts the MUVPN client by activating the security policy.
- The MUVPN client creates an encrypted tunnel to the Firebox® X Edge.
- The Firebox X Edge connects the remote computer to the trusted network. The employee now has secure remote access to the internal network.

The MUVPN client is available in two different packages. One version includes ZoneAlarm®, a personal software-based firewall. ZoneAlarm gives remote computers more security. The other package does not include ZoneAlarm. The use of ZoneAlarm is optional. Other than ZoneAlarm, the two packages are the same.

This chapter shows how to prepare the Firebox X Edge e-Series and the remote computer for a MUVPN connection. This chapter also includes information about the features of the ZoneAlarm personal firewall.

About This Chapter

You must complete some procedures to make sure that MUVPN operates correctly. Use this chapter to learn about these procedures:

- First, you must enable MUVPN on the Firebox® X Edge user's account and set the options that apply to all MUVPN clients. See “Enabling MUVPN for Firebox X Edge e-Series Users” on page 146 for information on the Firebox X Edge user's MUVPN account, and for information on MUVPN options that affect all MUVPN users.
- When the Firebox user's account is configured for MUVPN, the Firebox X Edge e-Series creates a configuration file (.wgx file). You must get this .wgx configuration file from the Edge. You also must download the MUVPN installation program from the WatchGuard® support site. See

"Distributing the Software and the .wgx File" on page 148 for information about how to get these items and how to give them securely to the remote user.

- The remote user's computer must have the correct networking components for MUVPN to operate correctly. See "Preparing Remote Computers for MUVPN" on page 149 to be sure that the user's computer is prepared to install and use MUVPN software.
- When the user has the MUVPN installation files and the .wgx configuration file, the user can install the MUVPN software. For more information, see "Installing and Configuring the MUVPN Client" on page 154.
- After the sections on how to set up the Firebox X Edge e-Series and the remote client, this chapter has sections on how to use the MUVPN software and how to use the ZoneAlarm personal firewall.
- You can use MUVPN to make the wireless network on the Firebox X Edge e-Series Wireless more secure. If you have an Edge Wireless, see "Using MUVPN on a Firebox X Edge e-Series Wireless Network" on page 161 for information about how to make the wireless computers use MUVPN on the Edge's wireless network.
- If you want to use a Pocket PC device to make a VPN connection to the Firebox X Edge e-Series, see "Tips for Configuring the Pocket PC" on page 162.
- At the end of this chapter is a section with troubleshooting tips.

Enabling MUVPN for Firebox X Edge e-Series Users

Before you configure the MUVPN client, you must configure MUVPN client and user settings on the Firebox® X Edge e-Series.

Configuring MUVPN client settings

Some MUVPN client settings apply to all Firebox X Edge MUVPN connections. Select **Firebox Users > Settings** to set these options:

- To make the .wgx file read-only so that the user cannot change the security policy file by default, select the **Make the MUVPN client security policy read-only** check box.
- Set how the virtual adapter operates on the client (Disabled, Preferred, or Required). The remote MUVPN computers can use a virtual adapter to get network settings, an IP address, and WINS and DNS address assignments. You can set the virtual adapter rule for your mobile users to:

Disabled

The mobile user does not use a virtual adapter to connect with the MUVPN client. This is the default setting. With the virtual adapter disabled, the MUVPN client is not assigned a WINS or DNS address. Because of this, the computer must have correct WINS and DNS addresses configured in the primary network card settings. See "Preparing Remote Computers for MUVPN" on page 149 for information on entering WINS and DNS addresses in the network card advanced settings.

Preferred

If the virtual adapter is in use or it is not available, the mobile user does not use a virtual adapter to connect with the MUVPN client.

If the virtual adapter is available, the remote computer is assigned the WINS and DNS addresses you entered in the **Firebox Users > Settings** area of the Firebox X Edge configuration pages.

Required

The mobile user must use a virtual adapter to connect with the MUVPN client. If the virtual adapter is not available on the MUVPN client computer, the VPN tunnel cannot connect.

The remote computer is assigned WINS and DNS addresses you entered in the **Firebox Users > Settings** area of the Firebox X Edge configuration pages.

- Type the IP addresses of the DNS and WINS servers for the MUVPN clients.

For more information, see "Configuring MUVPN client settings" on page 112.

Enabling MUVPN access for a Firebox user account

1 Add a new Firebox user or edit a Firebox user, as described in "Using Local Firebox Authentication" on page 113.

2 Click the **MUVPN** tab.

3 Select the **Enable MUVPN for this account** check box.

4 Type a shared key in the related field.
The .wgx file is encrypted with this shared key. The user enters the shared key when the .wgx file is imported. Do not give the shared key to any user that is not authorized to use this Firebox user account.

5 Type the virtual IP address in the related field.
The virtual IP address must be an address on the Firebox X Edge trusted network that is not used. This address is used by the remote computer to connect to the Firebox X Edge.

6 From the **Authentication Algorithm** drop-down list, select the type of authentication.
The options are MD5-HMAC and SHA1-HMAC.

7 From the **Encryption Algorithm** drop-down list, select the type of encryption.
The options are DES-CBC and 3DES-CBC.

8 Set MUVPN key expiration in kilobytes and/or hours. The default values are 8192 KB and 24 hours.
To remove a size and/or time expiration, set the value to zero (0).

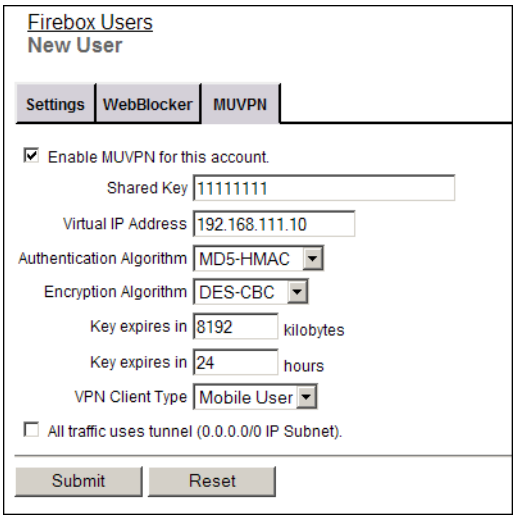
9 From the **VPN Client Type** drop-down list, select **Mobile User** if the remote user is connecting from a desktop or laptop computer instead of a handheld device such as a Pocket PC.

10 Select the **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** check box if the remote client sends all its traffic (including usual Web traffic) through the VPN tunnel to the Firebox X Edge. This also can let the MUVPN client connect with other networks that the Edge connects to.

If you do not select this check box, the remote user can connect with the Firebox X Edge trusted network only. You must enable this check box for the remote user to be able to connect to:

- Networks on the other side of a Branch Office VPN tunnel that the Edge has connected.
- Computers on the Edge's optional network.
- Networks that are behind a static route on the trusted or optional interface. For more information, see "Making Static Routes" on page 57.

11 Click **Submit**.



Configuring the Edge for MUVPN clients using a Pocket PC

To create a MUVPN tunnel between the Firebox X Edge e-Series and your Pocket PC, you must configure the Firebox User account differently. Follow the previous procedure, but select **Pocket PC** from the **VPN Client Type** drop-down list.

Note

WatchGuard® does not distribute a MUVPN software package for Pocket PCs. You must examine the software manufacturer's instructions to configure their software and the Pocket PC. For more information, see "Tips for Configuring the Pocket PC" on page 162.

Distributing the Software and the .wgx File

You must give the remote user the MUVPN software installer and the end-user profile, or .wgx file.

Get the MUVPN installation files from the WatchGuard Web site

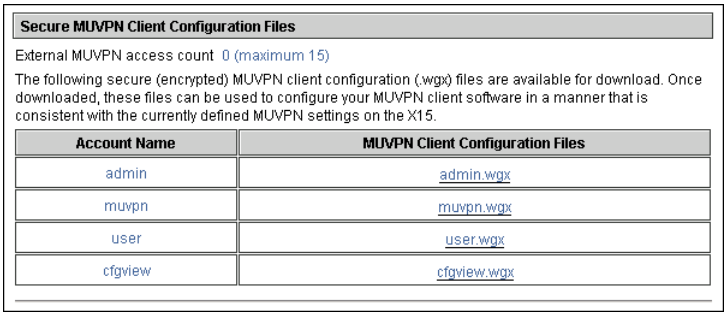
You must log in to the LiveSecurity® Service at http://www.watchguard.com/support to download the software. After you log in, go to the Latest Software area and select Firebox® X Edge in the **Choose Product Family** area. There are two different versions of Mobile User VPN software. One version contains the ZoneAlarm® personal firewall and the other one does not.

Get the user's .wgx file

The Firebox X Edge has encrypted MUVPN client configuration (.wgx) files available for download.

- To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
  The default URL is: https://192.168.111.1
- From the navigation bar, select **Firebox Users**.
- Below **Secure MUVPN Client Configuration Files**, select the .wgx file to download by clicking on the link `username.wgx` where `username` is the Firebox user's name.

- At the prompt, save the .wgx file to your computer.


Secure MUVPN Client Configuration Files
External MUVPN access count 0 (maximum 15)
The following secure (encrypted) MUVPN client configuration (.wgx) files are available for download. Once downloaded, these files can be used to configure your MUVPN client software in a manner that is consistent with the currently defined MUVPN settings on the X15.
Account Name
MUVPN Client Configuration Files
admin
admin.wgx
muvpn
muvpn.wgx
user
user.wgx
cfgview
cfgview.wgx

Give these two files to the remote user

Give the MUVPN software, and the .wgx file to the remote user. You also must give the user the shared key you used when you enabled the Firebox User account to use MUVPN, as described in "Enabling MUVPN for Firebox X Edge e-Series Users" on page 146. The user uses this shared key at the end of the installation process.

Note

The shared key is highly sensitive information. For security reasons, we recommend that you do not give the user the shared key in an e-mail. Because e-mail is not secure, an unauthorized user can get the shared key. Give the user the shared key by telling it to the user, or by some other method that does not allow an unauthorized person to get the shared key.

Preparing Remote Computers for MUVPN

You can install the MUVPN client only on computers that have these minimum requirements:

- A computer with a Pentium processor (or equivalent)
- Compatible operating systems and minimum RAM:
  - Microsoft Windows NT 4.0 Workstation: 32 MB
  - Microsoft Windows 2000 Professional: 64 MB
  - Microsoft Windows XP: 64 MB
- No other IPSec VPN client software can be on the computer. Remove any other software from the user's computer before you try to install the WatchGuard® MUVPN software.
- We recommend that you install the most current service packs for each operating system.
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 5.0 or later
- An Internet service provider account
- A dial-up or broadband (DSL or cable modem) connection

WINS and DNS servers

To use Windows file and print sharing on an MUVPN tunnel, the remote computer must connect to the WINS and DNS servers. These servers are on the Firebox® X Edge trusted network. To get to these serv-

ers, the IP addresses of the WINS and DNS servers must be configured on the remote computer or they must be assigned by the Edge when the VPN tunnel connects.

If the MUVPN client uses the virtual adapter, the WINS and DNS server IP addresses are assigned to the remote computer when the VPN tunnel is created.

If the MUVPN client does not use the virtual adapter, the remote computer must have your network's private WINS and DNS server IP addresses listed in the Advanced TCP/IP Properties of the primary Internet connection.

Windows NT setup

Use this section to install the network components for the Windows NT operating system. These components must be installed before you can use the MUVPN client on a Windows NT computer.

Installing Remote Access Services on Windows NT

You must install Remote Access Services (RAS) before you install the Mobile User VPN Adapter. To install RAS, use this procedure:

1 From the Windows desktop, select **Start > Settings > Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Click the **Services** tab and click the **Add** button.

4 Select **Remote Access Services** and click **OK**.
The Windows NT Setup dialog appears.

5 Type the path to the Windows NT installation files, or put your system installation CD in the computer and click **OK**.
The Remote Access Setup window appears.

6 Click **Yes** to add a RAS device, and then click **Add**.

7 Complete the Install New Modem wizard.

Note

If there is no modem installed, select the check box marked **Don't detect my modem; I will select it from a list**. Select the standard 28800 modem. If a modem is not available, you can select a serial cable between two computers.

8 Select the modem from the **Add RAS Device** window.

9 Click **OK**, click **Continue**, and click **Close**.

10 Restart the computer.

Configuring WINS and DNS settings on Windows NT

The remote computer must be able to contact the WINS servers and the DNS servers. These servers are found on the trusted network that is protected by the Firebox X Edge e-Series.

From the Windows desktop:

1 Select **Start > Settings > Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Click the **Protocols** tab and select the **TCP/IP** protocol.

4 Click **Properties**.
The Microsoft TCP/IP Properties window appears.

5 Click the **DNS** tab and click **Add**.

6 Type the IP address of your DNS server.
To add more DNS servers, repeat steps 5 and 6 for each server.

Note

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

7 Click the **WINS Address** tab, type the IP address of your WINS server in the applicable field, and then click **OK**.
You also can add a secondary or backup WINS server IP address.

8 Click **Close** to close the Network window.
The Network Settings Change dialog box appears.

9 Click **Yes** to restart the computer.
The computer restarts and your settings are applied.

Windows 2000 setup

Use this section to install and configure the network components for the Windows 2000 operating system. These components must be installed before you can use the MUVPN client on a Windows 2000 computer.

From the Windows desktop:

1 Select **Start > Settings > Network and Dial-up Connections**.

2 Right-click the connection you use to get Internet access and select **Properties**.
The connection properties window appears.

3 Click the **Networking** tab.

4 Make sure these components are installed and enabled:
To enable a component, click the adjacent check box. If a component is not installed, use the instructions to install it.
- Internet Protocol (TCP/IP)
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) network component on Windows 2000

From the connection window **Networking** tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Protocol** network component.
The Select Network Protocol window appears.

3 Below the **Microsoft** manufacturer, select the **Internet Protocol (TCP/IP)** network protocol and click **OK**.

Installing the File and Printer Sharing for Microsoft Networks on Windows 2000

From the connection window **Networking** tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Services** network component.
The Select Network Service window appears.

3 Below the **Microsoft** manufacturer, select the **File and Printer Sharing for Microsoft Networks** network service and click **OK**.

Installing the Client for Microsoft Networks on Windows 2000

From the connection window **Networking** tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Client** network component.
The Select Network Protocol window appears.

3 Select the **Client for Microsoft Networks** network client and click **OK**.

Configuring WINS and DNS settings on Windows 2000

The remote computer must be able to connect to the WINS and DNS servers. These servers are on the trusted network protected by Firebox X Edge e-Series.

From the connection window **Networking** tab:

1 Select the **Internet Protocol (TCP/IP)** component and click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.

2 Click **Advanced**.
The Advanced TCP/IP Settings window appears.

3 Click the **DNS** tab and from the section labeled **DNS server addresses, in order of use**, click **Add**.
The TCP/IP DNS Server window appears.

4 Type the IP address of the DNS server and click **Add**.
To add more DNS servers, repeat steps 3 and 4.

Note

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

5 Select the **Append these DNS suffixes (in order)** radio button and click **Add**.
The TCP/IP Domain Suffix window appears.

6 Type the domain suffix and click **Add**.
To add more DNS suffixes, repeat steps 5 and 6.

7 Click the **WINS** tab. From the section **WINS addresses, in order of use**, click **Add**.
The TCP/IP WINS Server window appears.

8 Type the IP address of the WINS server and click **Add**.
To add more WINS servers, repeat steps 7 and 8.

9 Click **OK** to close the Advanced TCP/IP Settings window. Click **OK** to close the Internet Protocol (TCP/IP) Properties window.

10 Click **OK** to close the connection properties window.

Windows XP setup

Use this section to install and configure the network components for the Windows XP operating system. You must install these components if you use the MUVPN client on a Windows XP computer.

From the Windows desktop:

1 Select **Start > Control Panel**
The Control Panel window appears.

2 Double-click the **Network Connections** icon.

3 Right-click the connection you use to get Internet access and select **Properties**.
The connection properties window appears.

4 Make sure these components are installed and enabled:
To enable a component, click the adjacent check box. If a component is not installed, follow the instructions to install it.

- Internet Protocol (TCP/IP)
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) Network Component on Windows XP

From the connection window **Networking** tab:

1. Click **Install**.
   The Select Network Component Type window appears.
2. Double-click the **Protocol** network component.
   The Select Network Protocol window appears.
3. Below the **Microsoft** manufacturer, select the **Internet Protocol (TCP/IP)** network protocol and click **OK**.

Installing the File and Printer Sharing for Microsoft Networks on Windows XP

From the connection window **Networking** tab:

1. Click **Install**.
   The Select Network Component Type window appears.
2. Double-click the **Services** network component.
   The Select Network Service window appears.
3. Below the **Microsoft** manufacturer, select the **File and Printer Sharing for Microsoft Networks** network service and click **OK**.

Installing the Client for Microsoft Networks on Windows XP

From the connection window **Networking** tab:

1. Click **Install**.
   The Select Network Component Type window appears.
2. Double-click the **Client** network component.
   The Select Network Protocol window appears.
3. Select the **Client for Microsoft Networks** network client and click **OK**.

Configuring WINS and DNS settings on Windows XP

The remote computer must be able to connect to the WINS and DNS servers. These servers are on the trusted network protected by the Firebox X Edge e-Series.

From the connection window **Networking** tab:

1. Select the **Internet Protocol (TCP/IP)** network component.
2. Click the **Properties** button.
   The Internet Protocol (TCP/IP) Properties window appears.
3. Click the **Advanced** button.
   The Advanced TCP/IP Settings window appears.
4. Click the **DNS** tab.
5. From the section labeled **DNS server addresses, in order of use**, click **Add**.
   The TCP/IP DNS Server window appears.
6. Type the IP address of the DNS server and click **Add**.
   To add more DNS servers, repeat steps 4 and 5.

Note

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

7 Select the **Append these DNS suffixes (in order)** radio button.

8 Below the radio button, click **Add**.
The TCP/IP Domain Suffix window appears.

9 Enter the domain suffix for your network's private domain and click **Add**.
To add more DNS suffixes, repeat steps 8 and 9.

10 Click the **WINS** tab.

11 From the section **WINS addresses, in order of use**, click **Add**.
The TCP/IP WINS Server window appears.

12 Type the IP address of the WINS server and click **Add**.
To add more WINS servers, repeat steps 11 and 12.

13 Click **OK** to close the Advanced TCP/IP Settings window. Click **OK** to close the Internet Protocol (TCP/IP) Properties window.

14 Click **OK** to close the connection window.

Installing and Configuring the MUVPN Client

Note

To install and configure the MUVPN client, you must have local administrator rights on the remote computer.

Installing the MUVPN client

To install the MUVPN client:

1 No other IPSec VPN client software can be active on the remote computer. Remove any other IPSec VPN software from the user's computer before installing the WatchGuard® MUVPN software.

2 Copy the MUVPN installation program and the .wgx file to the remote computer.

3 Double-click the MUVPN installation file to start the InstallShield wizard.

4 Click **Next**.
If the InstallShield shows a message about read-only files, click **Yes** to continue the installation.

5 A welcome message appears. Click **Next**.
The Software License Agreement appears.

6 Click **Yes** to accept the license agreement.
The Setup Type window appears.

7 Select the type of installation. We recommend that you use the **Typical** installation. Click **Next**.

8 On a Windows 2000 computer, the InstallShield looks for the Windows 2000 L2TP (Later 2 Tunneling Protocol) component. If the component is installed, the InstallShield does not install it again. Click **OK** to continue.
The Select Components window appears.

9 Do not change the default selections. Click **Next**.
The Start Copying Files window appears.

10 Click **Next** to install the files.
A command prompt window appears during the installation. The command prompt can stay for more than one minute. This is usual. After the file is installed, the command window closes automatically and the installation continues.

11 After the installation is complete, click **Finish**.

12 The InstallShield wizard looks for a user profile. Use the **Browse** button to find and select the folder containing the .wgx file. Click **Next**.
You can click Next at this step if you do not have the .wgx file at this time. You can import the .wgx file later. To import a .wgx file after the software is installed, double-click the .wgx file and type the shared key.

13 Click **OK** to continue the installation.

14 The MUVPN client is installed. Make sure the option **Yes, I want to restart my computer now** is selected. Click **Finish**.
The computer restarts.

Note

The ZoneAlarm personal firewall could prevent you from connecting to the network after the computer restarts. If this occurs, log on to the computer locally the first time after installation. For more information, see "The ZoneAlarm Personal Firewall" on page 159.

Uninstalling the MUVPN client

Use this procedure to remove the MUVPN client. We recommend that you use the Windows Add/Remove Programs tool.

1 Disconnect all existing tunnels and dial-up connections.

2 Deactivate the security policy on the client (see "Disconnecting the MUVPN client" on page 157).

3 Restart the remote computer.

4 From the Windows desktop, select **Start > Settings > Control Panel.**
The Control Panel window appears.

5 Double-click the **Add/Remove Programs** icon.
The Add/Remove Programs window appears.

6 Select **Mobile User VPN** and click **Change/Remove**.
The InstallShield wizard appears.

7 Select **Remove**. Click **Next**.
The Confirm File Deletion dialog box appears.

8 Click **OK** to remove all of the components.
A command prompt window appears during the procedure. This is usual. After the file is removed, the command prompt window closes automatically and the procedure continues.
The Uninstall Security Policy dialog box appears.

9 Click **Yes** to delete the security policy.
The InstallShield Wizard window appears.

10 Select **Yes, I want to restart my computer now**. Click the **Finish** button.
The computer restarts.

Note

The ZoneAlarm personal firewall settings are kept in these directories by default:
Windows NT and 2000: c:\winnt\internet logs\
Windows XP: c:\windows\internet logs
To remove these settings, delete the contents of the appropriate directory.

11 When the computer restarts, select **Start > Programs**.

12 Right-click **Mobile User VPN** and select **Delete** to remove this selection from your **Start** menu.

Connecting and Disconnecting the MUVPN Client

The MUVPN client software makes a secure connection from a remote computer to your protected network on the Internet. To start this connection, you must connect to the Internet and use the MUVPN client to connect to the protected network.

Connecting the MUVPN client

Start your connection to the Internet through a Dial-Up Networking connection, a LAN connection, or a WAN connection.

1 If the MUVPN client on the Windows desktop system tray is not active, right-click the icon and select **Activate Security Policy**.
For information about the MUVPN icon, see "The MUVPN client icon" on page 156.

2 From the Windows desktop, select **Start > Programs > Mobile User VPN > Connect**.
The WatchGuard Mobile User Connect window appears.

3 Click **Yes**.

The MUVPN client icon

The MUVPN icon appears in the Windows desktop system tray. The icon image gives information about the status of the connection.

Deactivated

The MUVPN Security Policy is not active. This icon can appear if the Windows operating system did not start a required MUVPN service. If this occurs, the remote computer must be restarted. If the problem continues, remove and install the MUVPN client again.

Activated

The MUVPN client can make a secure MUVPN tunnel connection.

Activated and Transmitting Unsecured Data

The MUVPN client is not connected to a secure MUVPN tunnel connection. The red bar on the right of the icon tells you that the client is sending data that is not secure.

Activated and Connected

The MUVPN client is connected with one or more secure MUVPN tunnels, but it is not sending data.

Activated, Connected, and Transmitting Unsecured Data

The MUVPN client started one or more secure MUVPN tunnel connections. The red bar on the right of the icon tells you that the client is sending data that is not secure.

Activated, Connected, and Transmitting Secured Data

The MUVPN client started one or more secure MUVPN tunnels. The green bar on the right of the icon tells you that the client is only sending data that is secure.

Activated, Connected, and Transmitting both Secured and Unsecured Data

The MUVPN client started one or more secure MUVPN tunnels. The green and red bars on the right of the icon tell you that the client is sending data that is secure and data that is not secure.

Allowing the MUVPN client through a personal firewall

To create the MUVPN tunnel, you must allow these programs through the personal firewall:

- MuvpnConnect.exe
- IreIKE.exe

The ZoneAlarm personal firewall detects when these programs try to get access to the Internet. A New Program alert window appears to request access for the MuvpnConnect.exe program.

From the New Program alert window:

1. Select the **Remember this answer the next time I use this program** check box and click **Yes**.
   This option makes the ZoneAlarm personal firewall allow Internet access for this program each time you start a MUVPN connection.
   The New Program alert window appears to request access for the IreIKE.exe program.
2. Set the **Remember this answer the next time I use this program** check box and click **Yes**.
   This option makes the ZoneAlarm personal firewall allow Internet access for this program each time you start a MUVPN connection.

Disconnecting the MUVPN client

From the Windows desktop system tray:

1. Right-click the MUVPN client icon and select **Deactivate Security Policy**.
   The MUVPN client icon with a red bar is shown.
2. If the ZoneAlarm personal firewall is active, deactivate it now by following the subsequent instructions.

From the Windows desktop system tray:

1. Right-click the ZoneAlarm icon shown at right.

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.
3 Click **Yes**.

Monitoring the MUVPN Client Connection

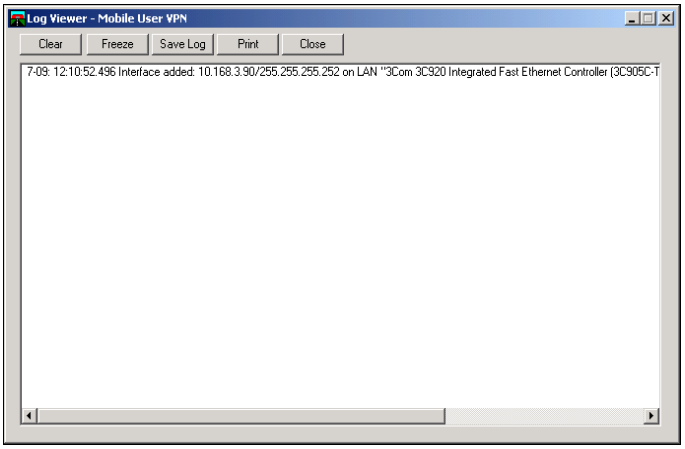
The Log Viewer and the Connection Monitor are installed with the MUVPN client. These tools let you monitor the MUVPN connection and troubleshoot problems.

Using Log Viewer

Use Log Viewer to show the connections log. This shows the events that occur when the MUVPN tunnel is started.

From the Windows desktop system tray:

1 Right-click the **Mobile User VPN** client icon.
2 Select **Log Viewer**.
The Log Viewer window appears.



Using Connection Monitor

The Connection Monitor shows statistical and diagnostic information for connections in the security policy. This window shows the security policy settings and the security association (SA) information. The monitor records the information that appears in this window during the phase 1 IKE negotiations and the phase 2 IPSec negotiations.

From the Windows desktop system tray:

1 Right-click the **Mobile User VPN** client icon.
2 Select **Connection Monitor**.
The Connection Monitor window appears.

An icon appears to the left of the connection name:

- SA tells you that the connection only has a phase 1 SA. A phase 1 SA is assigned in these situations:

  - for a connection to a secure gateway tunnel
  - when a phase 2 SA connection has not been made at this time
  - when a phase 2 SA connection cannot be made
- A key tells you that the connection has a phase 2 SA. This connection also can have a phase 1 SA.
- An animated black line below a key tells you that the client is sending or receiving secure IP traffic.
- A single SA icon with more than one key icon above it shows a single phase 1 SA to a gateway that protects more than one phase 2 SAs.

The ZoneAlarm Personal Firewall

ZoneAlarm® Personal firewall protects your computer and network with a simple rule: Block all incoming and outgoing traffic unless you explicitly allow that traffic for trusted programs.

When you use ZoneAlarm, you frequently see New Program alert windows. This alert appears when a software application tries to get Internet or local network access. This alert stops data from your computer without your authorization.

The ZoneAlarm personal firewall includes a tutorial after the MUVPN client is installed. Read the tutorial to learn how to use this software application.

For more information about the features and configuration of ZoneAlarm, use the ZoneAlarm help system. To get access to the help system, select **Start > Programs > Zone Labs > ZoneAlarm Help**.

Allowing traffic through ZoneAlarm

When a software application tries to get access through the ZoneAlarm personal firewall, a New Program alert appears. This alert tells the user the name of the software application. This can cause confusion for users.

To let a program get access to the Internet each time the software application is started, select the **Remember the answer each time I use this program** check box.

Here is a list of some programs that must go through the ZoneAlarm personal firewall when you use their associated software applications.

Programs That Must Be Allowed	
MUVPN client	IreIKE.exe MuvpnConnect.exe
MUVPN Connection Monitor	CmonApp.exe
MUVPN Log Viewer	ViewLog.exe
Programs That Can be Allowed	
MS Outlook	OUTLOOK.exe
MS Internet Explorer	IEXPLORE.exe
Netscape 6.1	netscp6.exe
Opera Web browser	Opera.exe
Standard Windows network applications	lsass.exe services.exe svchost.exe winlogon.exe

Shutting down ZoneAlarm

From the Windows desktop system tray:

1 Right-click the ZoneAlarm icon shown at right.

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.

3 Click **Yes**.

Uninstalling ZoneAlarm

From the Windows desktop:

1 Select **Start > Programs > Zone Labs > Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.

2 Click **Yes**.
The ZoneLabs TrueVector service dialog box appears.

3 Click **Yes**.
The Select Uninstall Method window appears.

4 Make sure **Automatic** is selected and then click **Next**.

5 Click **Finish**.

Note

The Remove Shared Component window can appear. During the initial installation of ZoneAlarm, some files were installed that can be shared by other programs on the system. Click **Yes to All** to completely remove all of these files.

6 The Install window appears and tells you to restart the computer. Click **OK** to restart.

Using MUVPN on a Firebox X Edge e-Series Wireless Network

You must protect your wireless network from unauthorized access because the signal can go out of your building. If you do not protect your network, unauthorized users can break into your network or make use of your Internet connection.

Some wireless network cards cannot use the stronger Wi-Fi Protected Access (WPA) encryption and instead use weaker Wired Equivalent Privacy (WEP) to secure the data that goes through the airwaves.

You can increase the security of your wireless network when you make the wireless computer users authenticate as MUVPN clients. This makes the Firebox® X Edge e-Series restrict traffic through the firewall unless the wireless computer has connected using an MUVPN tunnel.

To make sure wireless computers authenticate as MUVPN clients:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Network > Wireless**.

3 Select the check box **Require encrypted MUVPN connections for wireless clients**.

4 Click **Submit**.

Now you must decide which networks the wireless computers can connect with. When the wireless computers must authenticate as MUVPN clients, you can allow the computers to connect to:

Trusted network only

The wireless MUVPN client cannot connect to the Internet, the computers on the optional network, or any other network that the Firebox X Edge has a connection to.

All networks

This is the usual configuration for wireless MUVPN clients. The wireless MUVPN client can connect to:

- The trusted network
- The optional network
- Networks behind static routes
- Networks on the other side of a Branch Office VPN
- The external network (usually the Internet)

You can configure some Firebox X Edge users to connect only to the trusted network, and other Edge users to connect to all networks:

1 To allow a Firebox X Edge user to connect only to the trusted network, clear or do not select the check box **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** in the user's MUVPN setup.

2 To allow a Firebox X Edge user to connect to all networks through the VPN tunnel, select the check box **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** in the user's MUVPN setup.

To make wireless computers authenticate as MUVPN clients:

1 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1.

2 From the navigation bar, select **Network > Wireless**.

3 Select the check box **Require encrypted MUVPN connections for wireless clients**.

4 Click **Submit**.

Tips for Configuring the Pocket PC

WatchGuard® does not supply a Mobile User VPN software package for the Pocket PC platform. You must use the software manufacturer's instructions to configure their software and the Pocket PC.

The Firebox® X Edge e-Series allows only connections that use IPSec. The Edge does not support PPTP VPN tunnels.

Here are some configuration tips for the Pocket PC.

Phase 1 configuration of the Pocket PC's VPN software

- The Pocket PC's "IPSec Peer Gateway Address" must be the Firebox X Edge external IP address if the Pocket PC is connecting from the Internet.
- The IPSec Peer Gateway Address must be the Edge's private IP address if the Pocket PC is connecting from the optional or trusted network.
- The Phase 1 ID type must be "ID_USER_FQDN".

  This is known also as the IKE ID by some ISPs. The ID Type can also be known as the "Fully Qualified Username" or "User Name."
- The Phase 1 ID must be the Firebox X Edge user's name.
- You must use Aggressive Mode, not Main Mode.
- Extended authentication is not supported on the Firebox X Edge.
- Certificates are not supported on the Firebox X Edge.
- NAT Traversal is supported on the Firebox X Edge.
  Some implementations of the protocol require that you disable NAT Traversal on the Pocket PC.
- IKE-Config Mode is supported on the Firebox X Edge.
  Some IPSec software providers call this IKE Mode-Configuration.
- Phase 1 encryption type can be set to DES or 3DES. The Firebox X Edge uses DES as the default encryption.
- Phase 1 authentication type can be set to SHA1-HMAC or MD5-HMAC. The Firebox X Edge uses SHA1-HMAC as the default authentication.
- The Diffie-Hellman Group can be set to Group 1 or 2. The Firebox X Edge uses Group 1 as the default value.
- The Firebox X Edge accepts most Phase 1 time-out values.

Phase 2 configuration of the VPN

- The encryption algorithm and the authentication algorithm are configured in the Firebox User account settings, on the **MUVPN** tab.
- The IPSec Phase 2 timeouts are configured in the Firebox User account settings, on the **MUVPN** tab.
- The remote user's virtual IP address is configured in the Firebox User account settings, on the **MUVPN** tab. The virtual IP address must be an IP address from the Edge's trusted or optional network that is not being used.
- The Firebox X Edge does not support compression.
- By default, the network that the Firebox X Edge allows encrypted traffic to is the trusted network. The default trusted network is 192.168.111.0/24, or 192.168.111.0 with subnet mask 255.255.255.0.
- If all traffic from the Pocket PC must flow through the VPN, select the check box **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** in the user's MUVPN setup.

Troubleshooting Tips

You can get more information about the MUVPN client from the WatchGuard® web site:
http://www.watchguard.com/support

This section includes the answers to some frequently asked questions about the MUVPN client:

My computer hangs immediately after installing the MUVPN client.

This can be caused by one of two problems:

- The ZoneAlarm® personal firewall software application is stopping usual traffic on the local network.
- The MUVPN client is active and cannot create VPN tunnels.

When the MUVPN client is not in use, ZoneAlarm and the MUVPN client must be set to be not active.

From the Windows desktop system tray:

1. Restart your computer.
2. Right-click the MUVPN client icon and select **Deactivate Security Policy**.
   The MUVPN client icon with a red bar appears to show that the security policy is not active.
3. Right-click the ZoneAlarm icon shown at right.
4. Select **Shutdown ZoneAlarm**.
   The ZoneAlarm dialog box appears.
5. Click **Yes**.

I must enter my network login information even when I am not connected to the network.

When you start your computer, you must type your Windows network user name, password, and domain. It is very important that you type this information correctly. Windows keeps this information for use by network adapters and network applications. When you connect through the MUVPN client, your computer uses this information to connect to the company network.

I am not asked for my user name and password when I turn my computer on.

The ZoneAlarm personal firewall application can cause this problem. ZoneAlarm keeps your computer secure from unauthorized incoming and outgoing traffic. It also can prevent your computer from sending its network information. This prevents your computer from sending the login information. Make sure you turn off ZoneAlarm each time you disconnect the MUVPN connection.

Is the MUVPN tunnel working?

The MUVPN client icon appears in the Windows desktop system tray when the software application is started. The MUVPN client shows a key in the icon when the client is connected.

To test the connection, ping a computer on your company network.

- Select **Start > Run**. Type `cmd` and click **OK**. At the command prompt, type `ping` and the IP address of a computer on your company network.

My mapped drives have a red X through them.

Windows NT and 2000 examine and map network drives automatically when the computer starts. Because you cannot create a remote session with the company network before the computer starts, this procedure fails, which causes a red X to appear on the drive icons. To correct this problem, start a MUVPN tunnel and open the network drive. The red X for that drive disappears.

How do I map a network drive?

Because of a Windows operating system limitation, mapped network drives must be mapped again when you work remotely. To map a network drive again from the Windows desktop:

1 Right-click **Network Neighborhood**.

2 Select **Map Network Drive**.
The Map Network Drive window appears.

3 Use the drop-down list to select a drive letter.
Select a drive from the drop-down list or type a network drive path.

4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you select the **Reconnect at Logon** check box, the mapped drive appears when you start your computer only if the computer is directly connected to the network.

I am sometimes prompted for a password when I am browsing the company network.

Because of a Windows networking limitation, remote user VPN products can allow access only to a single network domain. If your company has more than one network connected together, you can browse only your own domain. If you try to connect to other domains, a password prompt appears. Unfortunately, even if you give the correct information, you cannot get access to these other networks.

It takes a very long time to shut down the computer after using the MUVPN client.

If you get access to a mapped network drive during an MUVPN session, the Windows operating system does not shut down until it gets a signal from the network.

I lost the connection to my ISP, and now I cannot use the company network.

If your Internet connection is interrupted, the connection to the MUVPN tunnel could stop. Use the procedure to close the tunnel. Reconnect to the Internet, then restart the MUVPN client.

APPENDIX A

Firebox X Edge e-Series Hardware

The WatchGuard® Firebox® X Edge e-Series is a firewall for small organizations and branch offices. The Firebox X Edge e-Series product line includes:

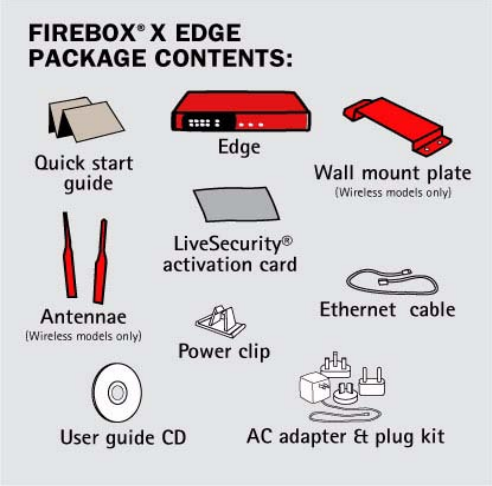
- Firebox X Edge e-Series
- Firebox X Edge e-Series Wireless

Package Contents

The Firebox® X Edge e-Series package includes:

- Hardware firewall
- *Firebox X Edge e-Series User Guide* on CD-ROM
- Firebox X Edge e-Series *Quick Start Guide*
- LiveSecurity® Service activation card
- Hardware warranty card
- AC adapter (12V/1.2A) with international plug kit
- Power cable clip, to attach to the cable and connect to the side of the Edge. This decreases the tension on the power cable.
- One straight-through cable
- Wall mount plate (wireless models only)

- Two antennae (wireless models only)



Specifications

The specifications for the Firebox® X Edge e-Series and the Firebox X Edge e-Series Wireless are:

Processor	X Scale (ARM)
CPU	266 MHz
Memory: Flash	64 MB
Memory: RAM	128 MB
Ethernet interfaces	6 each 10/100
Serial ports	1 DB9
Power supply	12V/1.2A
Operating temperature	0 - 40 C
Environment	Indoor use only
Dimensions for Firebox X Edge e-Series	Depth = 6.25 inches Width = 7.4 inches Height = 1.25 inches
Dimensions for Firebox X Edge e-Series Wireless, including antenna	Depth = 6.25 inches Width = 10.9 inches Height = 1.25 inches
Weight of Firebox X Edge e-Series	1.9 U.S. pounds
Weight of Firebox X Edge e-Series Wireless	2.0 U.S. pounds

Hardware Description

The Firebox® X Edge e-Series has a simple hardware architecture. All indicator lights are on the front panel and all ports and connectors are on the rear panel of the device.

Front panel

The front panel of the Firebox X Edge e-Series has 18 indicator lights to show link status. The top indicator light in each pair comes on when a link is made and flashes when traffic goes through the related interface. The bottom indicator light in each pair comes on when the link speed is 100 Mbps. If the bottom indicator light does not come on, the link speed is 10 Mbps.

WAN 1, 2

Each WAN indicator shows the physical connection to the external Ethernet interfaces. The light is yellow when traffic goes through the related interface.

WAP

The WAP indicator shows that the Firebox X Edge e-Series is activated as a wireless access point. The light is green when traffic goes through the wireless interface on a Firebox X Edge e-Series Wireless model.

Fail/Over

The Fail/Over indicator shows a WAN failover. The light is green when there is a WAN failover from WAN1 to WAN2. The light goes off when the external interface connection goes back to WAN1.

Link

The link indicator shows a physical connection to a trusted Ethernet interface. The trusted interfaces have the numbers 0 through 2. The light comes on when traffic goes through the related interface.

100

When a trusted network interface operates at 100 Mbps, the related 100 indicator light comes on. When it operates at 10 Mbps, the indicator light does not come on.

Status

The status indicator shows a management connection to the Firebox X Edge e-Series. The light goes on when you use your browser to connect to the Firebox X Edge e-Series configuration pages. The light goes off a short time after you close your browser.

Mode

The mode indicator shows the status of the external network connection. The light comes on when the Ethernet cable is correctly connected to the WAN1 interface. The light is green if the

Firebox X Edge e-Series can connect to the external network and send traffic. The light flashes if the Firebox X Edge e-Series cannot connect to the external network and send traffic.

Attn

The Attn indicator will light when you reset the Firebox X Edge e-Series to factory default settings.

Power

The power indicator shows that the Firebox X Edge e-Series is on.

Rear view

Ethernet interfaces LAN0 through LAN2

The Ethernet interfaces with the marks LAN0 through LAN2 are for the trusted network.

OPT interface

This Ethernet interface is for the optional network.

WAN interfaces 1 and 2

The WAN1 and WAN2 interfaces are for external networks.

Power input

A 12V/1.2A power supply is included with your Firebox X Edge e-Series. Connect the AC adapter to the Firebox X Edge and to a power source. The power supply tip is plus (+) polarity.

RESET button

To reset the Firebox X Edge e-Series, use the procedure in "Factory Default Settings" on page 33.

Side panels

Computer lock slot

There is a slot for a computer lock on the two side panels of the Firebox X Edge e-Series.

Antennae (wireless model only)

There are wireless antennae on the two side panels of the Firebox X Edge e-Series Wireless models.

Wall mounting plate (wireless model only)

The wall mounting plate enables you to put the Firebox X Edge e-Series in a good location to increase the range.

AC Power Adapter

The AC power adapter supplies power for the Firebox X Edge e-Series. You must use the correct plug for the AC power adapter for the power source used in your country.

The international plug kit includes four plugs: Q-NA (North America), Q-UK (United Kingdom), Q-EU (European Union), and Q-SAA (Asia).

Removing a plug from the AC power adapter

If the plug installed in the AC power adapter does not match your power source:

1 Use your thumb or finger to move the locking key on the AC power adapter down.

2 Hold the bottom of the plug.

3 Pull up from the bottom of the plug to remove it from the AC power adapter.

Connecting a plug to the AC power adapter

To install a different plug in the AC power adapter:

1 Put the top of the new plug in the AC power adapter at a 45-degree angle.
You must put in the top of the new plug first. Do not use force to put the plug into the adapter.

2 Push the bottom of the new plug into the AC power adapter.
The plug clicks into position.

About the Firebox X Edge e-Series Wireless.

The Firebox X Edge e-Series Wireless conforms to IEEE 802.11g/b wireless LAN standards. Some key features that have an effect on performance of an 802.11g/b wireless device include antenna directional gain, signal attenuation (path loss), and channel data rate.

Antenna directional gain

Antenna directional gain is based on the shape of the radiation pattern around the antenna. The Firebox X Edge e-Series Wireless uses two 5.1 dBi swivel-mount whip antennas. The whip antenna has a radiation pattern similar to a sphere that is squashed in the center. If the antenna points up, the gain is largest in the horizontal direction and less in the vertical direction.

Signal attenuation

Signal attenuation refers to the loss of signal power. It can be caused by multi-path reflection. Multi-path reflection occurs when RF signals that come to the receiver must move along more than one path because of walls and other surfaces between the transmitter and the receiver. It changes based on the phase at which the signals come, but signal strength can be increased or decreased by as much as 30dB.

To decrease the effect of multi-path reflection, the Firebox X Edge e-Series Wireless uses two antennas spaced some distance apart. This decreases signal cancellation and allows the software to find the best antenna to receive and transmit as conditions change.

Wireless clients usually have one antenna and are more sensitive to the effects of antenna location. Because of this, the Firebox X Edge e-Series Wireless can receive signals from a wireless client even if the client does not receive signals from the Firebox X Edge.

Channel data rate

Channel data rate changes with the modulation type, which changes based on conditions including noise and the distance between transmitter and receiver. In general, the available data rates for an IEEE 802.11g/b device change from 1 Mbps in the worst conditions to 54 Mbps in the best conditions

APPENDIX B

Legal Notifications

Copyright, Trademark, and Patent Information

General Information

Copyright© 1998 - 2006 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, Firebox, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT®, Windows® 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

OpenSSL

Copyright © 1998-2005 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

OpenLDAP

The OpenLDAP Public License Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Lua

Copyright © 2003-2004 Tecgraf, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NCFTP

The Clarified Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Distribution fee" is a fee you charge for providing a copy of this Package to another party.

"Freely Available" means that no fee is charged for the right to use the item, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain, or those made Freely Available, or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major network archive site allowing unrestricted access to them, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

e) permit and encourage anyone who receives a copy of the modified Package permission to make your modifications Freely Available in some specific way.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

e) offer the machine-readable source of the Package, with your modifications, by mail order.

5. You may charge a distribution fee for any distribution of this Package. If you offer support for this Package, you may charge any fee you choose for that support. You may not charge a license fee for the right to use this Package itself. You may distribute this Package in aggregate with other (possibly commercial and

possibly nonfree) programs as part of a larger (possibly commercial and possibly nonfree) software distribution, and charge license fees for other parts of that software distribution, provided that you do not advertise this Package as a product of your own. If the Package includes an interpreter, You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of the Standard Version of the Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

DHCP

Copyright © 1995, 1996, 1997, 1998, 1999 The Internet Software Consortium. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of The Internet Software Consortium nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software has been written for the Internet Software Consortium by Ted Lemon <mellon@fugue.com> in cooperation with Vixie Enterprises. To learn more about the Internet Software Consortium, see ``http://www.vix.com/isc". To learn more about Vixie Enterprises, see ``http://www.vix.com".

This client was substantially modified and enhanced by Elliot Poger for use on Linux while he was working on the MosquitoNet project at Stanford.

The current version owes much to Elliot's Linux enhancements, but was substantially reorganized and partially rewritten by Ted Lemon so as to use the same networking framework that the Internet Software Consortium DHCP server uses. Much system-specific configuration code was moved into a shell script so that as support for more operating systems is added, it will not be necessary to port and maintain system-specific configuration code to these operating systems - instead, the shell script can invoke the native tools to accomplish the same purpose.

bzip2

The program, "bzip2", the associated library "libbzip2", and all documentation, are copyright © 1996-2005 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

libexpat

Copyright © 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper.

Copyright © 2001, 2002, 2003 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

lsof

Copyright 1994 Purdue Research Foundation, West Lafayette, Indiana 47907. All rights reserved.
Written by Victor A. Abell
This software is not subject to any license of the American Telephone and Telegraph Company or the Regents of the University of California.
Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it freely, subject to the following restrictions:
1. Neither the authors nor Purdue University are responsible for any consequences of the use of this software.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Credit to the authors and Purdue University must appear in documentation and sources.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. This notice may not be removed or altered.

libarchive

Copyright © 2003-2004 Tim Kientzle All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer in this position and unchanged.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

zlib

© 1995-2004 Jean-loup Gailly and Mark Adler
This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.
Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:
1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

sasl

Copyright © 1998-2003 Carnegie Mellon University. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact

Office of Technology Transfer
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890
(412) 268-4387, fax: (412) 268-7395
tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

pppd

pppd has many licenses. This includes the GPL, the LGPL, SUN license, RSA license, public domain, and several BSD licenses that require separate attributions.

One or more of the following may apply to any one module:

1. chat, chatchat.c and sha1.[ch] are public domain
2. The Gnu Public License
3. The Gnu Lesser Public License

Copyright © 1990, RSA Data Security, Inc. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

eap.h - Extensible Authentication Protocol for PPP (RFC 2284)

Copyright © 2001 by Sun Microsystems, Inc. All rights reserved.

Non-exclusive rights to redistribute, modify, translate, and use this software in source and binary forms, in whole or in part, is hereby granted, provided that the above copyright notice is duplicated in any source form, and that neither the name of the copyright holder nor the author is used to endorse or promote products derived from this software.
THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Original version by James Carlson

Copyright © 2002 Roaring Penguin Software Inc.
Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Roaring Penguin Software Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Roaring Penguin Software Inc.
Roaring Penguin Software Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright © 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>
Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.
Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1992 Livingston Enterprises, Inc.
Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566
Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.
Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

© The Regents of the University of Michigan and Merit Network, Inc.
1992, 1993, 1994, 1995 All Rights Reserved
Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.
THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE.

The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.
License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.
RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Copyright © 1995 Eric Rosenquist. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 1989 Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Van Jacobson (van@helios.ee.lbl.gov), Dec 31, 1989: Initial distribution.

Copyright © 1985, 1986 The Regents of the University of California. All rights reserved.
This code is derived from software contributed to Berkeley by James A. Woods, derived from original work by Spencer Thomas and Joseph Orost.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 1984-2000 Carnegie Mellon University. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact
Office of Technology Transfer
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890
(412) 268-4387, fax: (412) 268-7395
tech-transfer@andrew.cmu.edu
4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."
CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 1994-2002 Paul Mackerras. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
3. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Paul Mackerras <paulus@samba.org>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 1995 Pedro Roque Marques. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Pedro Roque Marques <pedro_m@yahoo.com>"

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 1999 Tommi Komulainen. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Tommi Komulainen <Tommi.Komulainen@iki.fi>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 2002 Google, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenNTPD

This is a summary of the licences for the files that make up Portable OpenNTPD. Apart from the exceptions listed below, all of the files are under an ISC-style licence with the following copyright holders, first for the files from OpenBSD's ntpd:

Henning Brauer, Alexander Guy

and the portability layer:

Darren Tucker, Damien Miller, Internet Software Consortium, Todd C. Miller, Anthony O.Zabelin

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF MIND, USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

bsd-snprintf.c is from OpenSSH and has the following licence:
Copyright Patrick Powell 1995
This code is based on code written by Patrick Powell (papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions.

uidswap.c is from OpenSSH and has the following licence:
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved
As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

The following files are from OpenSSH or OpenBSD and are under a 2-term BSD license with the noted copyright holders: atomicio.c, atomicio.h, bsd-poll.h: Theo de Raadt
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following files are from OpenSSH and are under a 3-term BSD license
with the noted copyright holders:
fake-rfc2553.c, fake-rfc2553.h: WIDE Project, Damien Miller.
daemon.c, sys-queue.h: The Regents of the University of California
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JFFS2, ProCPS, iputils

JFFS2, ProCPS, and iputils are licensed under the GNU Public License (GPL). Specific copyright information for each software program follows the text of the GPL.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
9 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.
When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for

this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license

would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright (C) 2001, 2002 Red Hat, Inc.

JFFS2 is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

JFFS2 is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
You should have received a copy of the GNU General Public License along with JFFS2; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.
As a special exception, if other files instantiate templates or use macros or inline functions from these files, or you compile these files and link them with other works to produce a work based on these files, these files do not by themselves cause the resulting work to be covered by the GNU General Public License. However the source code for these files must still be made available in accordance with section (3) of the GNU General Public License.
This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.
For information on obtaining alternative licences for JFFS2, see http://sources.redhat.com/jffs2/jffs2-licence.html

iputils contains several files with different licenses. Each file could be licensed under one or more of the following:
ping.c and pin6.c are Public Domain

Rdisc (this program) was developed by Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Rdisc without charge, and they may freely distribute it.
RDISC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.
Rdisc is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.
SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY RDISC OR ANY PART THEREOF.
In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.
Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California 94043

Copyright (c) 1989 The Regents of the University of California. All rights reserved.
This code is derived from software contributed to Berkeley by Mike Muuss.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PCRE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 6 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2005 University of Cambridge All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2005, Google Inc. All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Traceroute

Copyright (c) 1988 Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

PSC Changes Copyright (c) 1992 Pittsburgh Supercomputing Center. All rights reserved.
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the modifications to this software were developed by the Pittsburgh Supercomputing Center. The name of the Center may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

DNS lookup portions of this code also subject to the following: Use the domain system to resolve a name.
Copyright (C) 1988,1990,1992 Dan Nydick, Carnegie-Mellon University
Anyone may use this code for non-commercial purposes as long as my name and copyright remain attached.

Redboot

Red Hat eCos Public License v1.1
1. DEFINITIONS
1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.
1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.
1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.
1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.
1.5. "Executable" means Covered Code in any form other than Source Code.
1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.
1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.
1.8. "License" means this document.
1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:
A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
B. Any new file that contains any part of the Original Code or previous Modifications.
1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or a list of source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1 <#section-6.1>. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

1.13. "Red Hat Branded Code" is code that Red Hat distributes and/or permits others to distribute under different terms than the Red Hat eCos Public License. Red Hat's Branded Code may contain part or all of the Covered Code.

2. SOURCE CODE LICENSE

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell ("Utilize") the Original Code (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to Utilize the Original Code (or portions thereof) and not to any greater extent that may be necessary to Utilize further Modifications or combinations.

2.2. Contributor Grant.

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Contributor, to Utilize the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to Utilize the Contributor Version (or portions thereof), and not to any greater extent that may be necessary to Utilize further Modifications or combinations.

3. DISTRIBUTION OBLIGATIONS

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available and to the Initial Developer; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party. You are responsible

for notifying the Initial Developer of the Modification and the location of the Source if a contact means is provided. Red Hat will be acting as maintainer of the Source and may provide an Electronic Distribution mechanism for the Modification to be made available. You can contact Red Hat to make the Modification available and to notify the Initial Developer. (http://sourceware.cygnus.com/ecos/)

3.3. Description of Modifications.

You must cause all Covered Code to which you contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If You have knowledge that a party claims an intellectual property right in particular functionality or code (or its utilization under this License), you must include a text file with the source code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If you obtain such knowledge after You make Your Modification available as described in Section 3.2, You shall promptly modify the LEGAL file in all copies You make available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Your Modification is an application programming interface and You own or control patents which are reasonably necessary to implement that API, you must also include this information in the LEGAL file.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code, and this License in any documentation for the Source Code, where You describe recipients' rights relating to Covered Code. If You created one or more Modification(s), You may add your name as a Contributor to the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then you must include such notice in a location (such as a relevant directory file) where a user would be likely to look for such a notice. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code.

However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2 <#section-3.2>. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

If you distribute executable versions containing Covered Code, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. INABILITY TO COMPLY DUE TO STATUTE OR REGULATION

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; (b) cite the statute or regulation that prohibits you from adhering to the license; and (c) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 <#section-3.4> and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it. You must submit this LEGAL file to Red Hat for review, and You will not be able use the covered code in any means until permission is granted from Red Hat to allow for the inability to comply due to statute or regulation.

5. APPLICATION OF THIS LICENSE

This License applies to code to which the Initial Developer has attached the notice in Exhibit A <#exhibit-a>, and to related Covered Code.

Red Hat may include Covered Code in products without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

Red Hat may license the Source Code of Red Hat Branded Code without Red Hat Branded Code becoming subject to the terms of this License, and may license Red Hat Branded Code on different terms from those contained in this License. Contact Red Hat for details of alternate licensing terms available.

6. VERSIONS OF THE LICENSE

6.1. New Versions.

Red Hat may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Red Hat. No one other than Red Hat has the right to modify the terms applicable to Covered Code beyond what is granted under this and subsequent Licenses.

6.3. Derivative Works.

If you create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), you must (a) rename Your license so that the phrases "ECOS", "eCos", "Red Hat", "RHEPL" or any confusingly similar phrase do not appear anywhere in your license and (b) otherwise make it clear that your version of the license contains terms which differ from the Red Hat eCos Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION

This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the

Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

9. LIMITATION OF LIABILITY

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THAT EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in, the United States of America: (a) unless otherwise agreed in writing, all disputes relating to this License (excepting any dispute relating to intellectual property rights) shall be subject to final and binding arbitration, with the losing party paying all costs of arbitration; (b) any arbitration relating to this Agreement shall be held in Santa Clara County, California, under the auspices of JAMS/EndDispute; and (c) any litigation relating to this Agreement shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS

Except in cases where another Contributor has failed to comply with Section 3.4 <#section-3.4>, You are responsible for damages arising, directly or indirectly, out of Your utilization of rights under this License, based on the number of copies of Covered Code you made available, the revenues you received from utilizing such rights, and other relevant factors. You agree to work with affected parties to distribute responsibility on an equitable basis.

13. ADDITIONAL TERMS APPLICABLE TO THE RED HAT ECOS PUBLIC LICENSE

Nothing in this License shall be interpreted to prohibit Red Hat from licensing under different terms than this License any code which Red Hat otherwise would have a right to license.

Red Hat and logo - This License does not grant any rights to use the trademark Red Hat, the Red Hat logo, eCos logo, even if such marks are included in the Original Code. You may contact Red Hat for permission to display the Red Hat and eCos marks in either the documentation or the Executable version beyond that required in Exhibit B.

Inability to Comply Due to Contractual Obligation - To the extent that Red Hat is limited contractually from making third party code available under this License, Red Hat may choose to integrate such third party code

into Covered Code without being required to distribute such third party code in Source Code form, even if such third party code would otherwise be considered "Modifications" under this License.

EXHIBIT A

"The contents of this file are subject to the Red Hat eCos Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.redhat.com/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is eCos - Embedded Configurable Operating System, released September 30, 1998. The Initial Developer of the Original Code is Red Hat. Portions created by Red Hat are Copyright (C) 1998, 1999, 2000 Red Hat, Inc. All Rights Reserved."

EXHIBIT B

Part of the software embedded in this product is eCos - Embedded Configurable Operating System, a trademark of Red Hat. Portions created by Red Hat are Copyright (C) 1998, 1999, 2000 Red Hat, Inc. (http://www.redhat.com/). All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY RED HAT AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Certifications and Notices

WEEE Statement:

WEEE is a general set of requirements dictated in the EU Directive 2002/96/EC. This Directive mandated that member EU countries enact regulations governing the Waste of Electrical and Electronic Equipment (WEEE). The Directive, and its individual transpositions into specific country laws and legislation, is aimed at the reduction of WEEE through reuse, recovery, and recycling of WEEE.

WatchGuard® is working in partnership with our European Union (EU) distribution partners to ensure that our products are in compliance with the WEEE statutes, and that the recovery of our product per the specific EU country legislative requirements is seamless for our product's end users. If you have a WatchGuard product that is at its end of life and needs to be disposed of, please contact WatchGuard Customer Care Department at:

U.S. Customers: 877.232.3531
International Customers: +1.206.613.0456

WatchGuard is reasonably confident that our products do not contain any substances or hazardous materials presently banned by any legislation, and do not present a risk due to hazardous materials. WEEE recovery professionals should also note that these products do not have any materials that are of particular high value in their individual form.

RoHS Statement:

The member states of European Union approved directive 2002/95/EC, Restrictions of Hazardous Substances ("RoHS directive) that becomes valid on July 1, 2006. It states that all new electrical and electronic equipment put on the market within the member states must not contain certain hazardous materials. The WatchGuard Firebox X Edge e-Series will comply with the European

Union's R0HS directive 2002/95/EC and similar regulations that may be adopted by other countries for European Sales.

FCC Certification

This appliance has been tested and found to comply with limits for a Class A digital appliance, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This appliance may not cause harmful interference.
- This appliance must accept any interference received, including interference that may cause undesired operation.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Note

Changes or modifications to this equipment that are not expressly approved by WatchGuard could void the user's authority to operate the equipment.

Note

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Part 68 Statement (DSL Version)

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications to maintain uninterrupted service.

In the event the equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning. The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request that you remove the equipment from the network until the problem is resolved. This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU)

Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel broulleur du Canada.

CANADA RSS-210

The term "IC:" before the radio certification number only signifies that Industry of Canada technical specifications were met.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 5.1 dB. Antennas not included in this list or having a gain greater than 5.1 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

WGRD P/N 155-1305-002 or any antenna with
5.1dB or lower gain

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

France

Note

En France, ce produit ne peut être installé et opéré qu'à l'intérieur, et seulement sur les canaux 10, 11, 12 , 13 comme défini par IEEE 802.11g/b. L'utilisation de ce produit à l'extérieur ou sur n'importe quel autre canal est illégal en France.

Note

In France, this product may only be installed and operated indoors, and only on channels 10, 11, 12, 13 as defined by IEEE 802.11g/b. Use of the product outdoors, or on any other channel, is illegal in France.

Class A Korean Notice

사용자 안내문(A급 기기)
본 기기는 업무용으로 전자파적합등록을 받은 기기이오니,
만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로
교환 하시기 바랍니다.

VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（VCCI)の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Class A Notice

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，
可能會造成射頻干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

Taiwanese Wireless Notice

根據交通部 低功率管理辦法 規定：

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Declaration of Conformity

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):

Wireless Internet Firewall with VPN, Models XP2E6W, XP2E6,XP2A1E5

EU Directive(s):

Radio & Telecommunications Terminal Equipment (1999/5/EC)
Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

Common Standard(s):

EN60950-1 (December 2001) Safety of ITE

EN50022 (1998), Class A Emissions for ITE
EN50024 (1998) Immunity for ITE

Wireless Standard(s):

ETSI EN 300 328-02 V1.4.1 (2003-04) EMC and Radio Spectrum Matters
ETSI EN 301 489-17 V1.1.1 (2000-09) EMC and Radio Spectrum Matters
ETSI EN 301 489-01 V1.4.1 (2002-08) EMC and Radio Spectrum Matters

Signature
Full Name Edward Borey
Position Chairman, CEO
Date 07 February 2006

Limited Hardware Warranty

This Limited Hardware Warranty (the "Warranty") applies to the enclosed Firebox hardware product, not including any associated software which is licensed pursuant to a separate end-user license agreement and warranty (the "Product"). BY USING THE PRODUCT, YOU (either an individual or a single entity) AGREE TO THE TERMS HEREOF. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from which you purchased it for a full refund. WatchGuard Technologies, Inc. ("WatchGuard") and you agree as set forth below or on the reverse side of this card, as applicable:

1. LIMITED WARRANTY. WatchGuard warrants that upon delivery and for one (1) year thereafter (the "Warranty Period"): (a) the Product will be free from material defects in materials and workmanship, and (b) the Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard applicable specifications.
This warranty does not apply to any Product that has been: (i) altered, repaired or modified by any party other than WatchGuard except for the replacement or inclusion of specified components authorized in and performed in strict accordance with documentation provided by WatchGuard; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Product from the manufacturers of Product components. However, you agree not to look to WatchGuard for, and hereby release WatchGuard from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.
2. REMEDIES. If any Product does not comply with the WatchGuard warranties set forth in Section 1 above, WatchGuard will, following receipt of the product you claim is defective and at its option, either (a) repair the Product, or (b) replace the Product; provided, that you will be responsible for returning the Product and for all costs of shipping and handling. Repair or replacement of the Product shall not extend the Warranty Period. Any Product, component, part or other item replaced by WatchGuard becomes the property of WatchGuard. WatchGuard shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Products.
3. DISCLAIMER AND RELEASE. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR FROM PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE PRODUCT).
4. LIMITATION AND LIABILITY. WATCHGUARD'S LIABILITY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) WITH REGARD TO ANY PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS, OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY.
5. MISCELLANEOUS PROVISIONS. This Warranty will be governed by the laws of the state of Washington, U.S.A., without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sales of Goods, as amended, shall not apply. You agree not to directly or indirectly transfer the Product or associated documentation to any country to which such transfer would be prohibited by the U.S. Export laws and regulations. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be

modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard and you relating to the Product, and supersedes any prior purchase order, communications, advertising or representations concerning the Product AND BY USING THE PRODUCT YOU AGREE TO THESE TERMS. IF THE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS BY USING THE PRODUCT REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THE WARRANTY ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS WARRANTY; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THE WARRANTY AND PERFORM ITS OBLIGATIONS UNDER THE WARRANTY AND; (C) THE WARRANTY AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THE WARRANTY DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of the Warranty will be valid unless it is in writing and is signed by WatchGuard.

Symbols

.wgx files
    described 145
    distributing 148
    viewing available 26

Numerics

1-to-1 NAT. See NAT, 1-to-1

A

abbreviations used in guide v
Active Directory authentication 116—119
Add Gateway page 139
Add Route page 58
Add Traffic Control dialog box 96
Administration page
    described 26
    subpages of 26
Administrative Access levels 110
administrator account 115
Aggressive Mode 140
Allow access to the External Network check box 114
Allow access to VPN check box 114
Allowed Sites pages 132
antenna directional gain 170
authentication
    allowing internal hosts to bypass 120
    changing options for 110
    described 110
    process for 112

B

bandwidth, described 2
Blocked Sites page 89
broadband connections 2

C

cables
  connecting computer and Edge 15
  included in package 10, 165
channel bandwidth 170
channels, setting for wireless 68
CIDR notation 58, 82, 83, 141
Classless Inter Domain Routing 58, 82, 83, 141
Client for Microsoft Networks, installing 152
computers
  configuring to connect to Edge 17—18
  remote, preparing for MUVPN 149—154
  supported with Edge 9
configuration file, viewing 44
configuration pages
  description 22—30
  navigating 22—30
  opening 22
  whether Edge uses HTTP or HTTPS 26
Connection Monitor, using to monitor MUVPNs 158
custom incoming services, creating 80, 85
Custom Service page 81, 85

D

default factory settings 33—34
default gateway 4
Denied Sites page 133
devices
  connecting to 4+ 15
  maximum number of 16
DHCP
  described 4, 11, 46
  setting your computer to use 17
  using on the optional network 55
DHCP address reservations
  setting on the optional network 56
  setting on the trusted network 51
DHCP Address Reservations page 52, 56
DHCP relay
  configuring the optional network 56
  configuring the trusted network 52

DHCP server
configuring Firebox as 51, 55
Diffie-Hellman groups 140
Digital Subscriber Line (DSL) 2
DNS
described 4
dynamic DNS service 58
DVCP, described 136
Dynamic DNS client page 59
dynamic DNS service, registering with 58—60
Dynamic Host Configuration Protocol. See DHCP
dynamic IP addresses
and external network 46
described 4, 11
dynamic NAT. See NAT, dynamic
Dynamic VPN Configuration Protocol, described 136
DynDNS.org 58

E

echo host 142
Enable DHCP Relay check box 52
Enable DHCP Server on the Trusted Network check box 51
Enable Optional Network check box 54
external interface
configuring 46—49
configuring with Quick Setup Wizard 18—19
default setting for 33
described 7
if ISP uses DHCP 46
if ISP uses PPPoE 48
if ISP uses static addressing 47
network address for 10
External Network Configuration page 47, 48

F

factory default settings
described 33
resetting to 34
failover network. See WAN failover
File and Printer Sharing for Microsoft Networks 151
and Windows XP 153

Filter Traffic page 79, 83, 87
Firebox Users page 107, 108, 113, 115, 117, 119
  described 26
  subpages of 26
Firebox X Edge
  administrator account 115
  authenticating to 112
  back panel 168
  cabling 15
  configuring as DHCP server 51
  connecting to 4+ devices 15
  described 165
  front panel 167
  hardware description 167—168
  hardware specifications 166
  hardware specifications for 166
  installing 9—20
  lights on 167
  package contents 9, 165
  rear panel 168
  registering with LiveSecurity 20
  resetting to factory default 34
  restarting 34—35
  side panel 168
  upgrade options 42
  viewing log messages for 103
  Web pages. See configuration pages
Firebox X Edge Wireless
  and wireless guest services 72
  configuring encryption 70
  configuring wireless card 74
  controlling SSID broadcasts 68
  described 169
  hardware information for 169, 169—170
  logging 68
  physically connecting 65
  restricting by MAC address 71
  selecting wireless network assignment 67
  setting fragmentation threshold 69
  setting operating region 68
  setting the SSID 68
  setting up 65—75
  setting wireless authentication method 70
  setting wireless mode for 69
  using MUVPN on 161

Firewall Options page 89, 91
Firewall page
  described 27
  subpages of 27—28
firewalls, described 6
firmware, updating 41—42
FTP access, denying 90

G

gateway, default 4

H

hardware description 167—168
hardware information 165—170
hardware specifications 166
HTTP proxy settings, disabling 13
HTTP server port, changing 37
HTTP/HTTPS, using for Firebox management 37

I

incoming service, creating custom 80, 85
indicator lights 167
installation
  disabling TCP/IP proxy settings 13
  setting your computer to connect to Edge 17
  TCP/IP properties 11
installing the Firebox X Edge 9—20
Internet
  connecting to 2
  connection, required for Firebox X Edge 9
  how information travels on 3
Internet Protocol (TCP/IP) Network Component
  and Windows XP 153
Internet Protocol (TCP/IP) network component, installing 151
Internet Protocol (TCP/IP) Properties dialog box 17, 18
IP addresses
  changing with Network Setup Wizard 45
  described 3, 4

dynamic 11
giving your computer static 17
methods for assigning 10
static 11, 46

L

LDAP authentication 116—119
and MUVPNs 120
lights on front panel 167
LiveSecurity Service
and software updates 41
registering with 20
Local Area Network (LAN) 1
Log Authentication Events check box 68
log messages
contents of 103
viewing 103
Log Server, logging to 104
Log Viewer, using to monitor MUVPNs 158
logging
configuring ??—37, 103—??
described 103
to syslog host 105
viewing status of 28
Logging page
described 28, 104
subpages of 28

M

MAC address, restricting wireless access by 71
Manual VPN page 139
manual VPNs. See VPNs, manual
model upgrades 44
MUVPN client
allowing through personal firewall 157
configuring 145—159
configuring user settings for 112
connecting 156
described 145
disconnecting 157
enabling 146

icon for 156—157
installing 154
monitoring 158—159
preparing remote computers for 149—154
troubleshooting 163—164
uninstalling 155
MUVPN Clients upgrade 43
MUVPNs
and LDAP authentication 120
distributing .wgx files 148
enablng access for users 147
for clients using Pocket PCs 148
monitoring with Connection Monitor 158
monitoring with Log Viewer 158
system requirements for 149
using on wireless networks 161
WINS and DNS servers 149

N

NAT
1-to-1
configuring 99—101
described 98
configuring 98
described 97
dynamic
described 97
if Edge behind device that does 140
if your ISP uses 11
static 98
traversal 140
types of 97
NAT (Network Address Translation) page 99, 101
navigation bar 23
netmask 11
Network Address Translation. See NAT
network addresses, described 4, 10
Network page
described 25
subpages of 25
network security, described 1
Network Setup Wizard 45
network traffic. See traffic

networks, types of 1
New User page 113
numbered ports 168

O

operating region, setting for wireless 68
optional interface
  assigning static IP addresses on 57
  changing IP address of 54
  configuring 53—57
  configuring additional computers on 57
  default setting for 33
  described 7, 53
  enabling 54
  setting DHCP address reservations on 56
  using DHCP on 55
  using DHCP relay on 56
Optional Network Configuration page 54, 55, 56
options
  model upgrade 44
  MUVPN Clients 43
  seat license upgrade 43
  WAN failover 43
  WebBlocker 43

P

packets, described 3
passphrases, described 113, 115
path-loss 170
Perfect Forward Secrecy 141
Phase 1 settings 139
Phase 2 settings 141
ping requests, denying 90
Pocket PCs
  creating MUVPN tunnels to 148
  creating tunnels to 148
  tips for configuring 162
Point-to-Point Protocol over Ethernet. See PPPoE
port, changing HTTP server port 37
ports

numbered 168
numbering 5
trusted network 168
WAN 168
WAN1 60
WAN2 60
power cable clip 10, 165
power input 168
PPPoE
advanced settings for 48—49
described 4, 11, 46
settings for 12
profiles, creating WebBlocker 123—124
protocols
described 2
TCP/IP 2

Q

Quality of Service (QoS)
configuring 94—97
described 93
traffic categories for 93
Quick Setup Wizard
described 18
running 18—??

R

read-only administrative account 114
Remote Access Services, installing 150
remote management
enabling 38—??
enabling with WFS 40—41
RESET button 168
resetting to factory default 34
restarting 34—35
Restrict Access by Hardware Address check box 72
routes
configuring static 57
viewing 25
Routes page 58

S

seat licenses
  described 108
  upgrade 43
serial number, viewing 24
services
  creating custom 80—81, 85—86
  creating custom incoming 80, 85
  described 4, 77
  viewing current 27
Session idle time-out field 114
session licenses 16
Session maximum time-out field 114
sessions
  closing 108
  described 108
  idle timeout 114
  maximum timeout 114
  viewing current active 108
  viewing currently active 108
Settings page 110
shared secret 138
signal attenuation 170
sites, blocking 89
SSID (Service Set Identifier) 68
SSID broadcasts, controlling 68
static IP addresses
  and external network 46
  and VPNs 143
  described 4, 11
  obtaining 143
static NAT. See NAT, static
static routes
  making 57
  removing 58
subnet mask 11
SurfControl 121
syslog host, logging to 105
Syslog Logging page 105
syslog, described 105
system configuration pages. See configuration pages
System Status page
  described 22

green triangle on 24
information on 24
navigation bar 23
System Time page 36
system time, setting 35

T

TCP (Transmission Control Protocol) 2
TCP/IP
described 2
properties, determining 11—12
time zone
setting 35
setting with Quick Setup Wizard 19
To 99
traffic
categories of 94
causes for slow 93
described 93
high priority 94
interactive 94
logging all outbound 90
low priority 94
managing 93—97
medium priority 94
traffic control filter, defining 96
Traffic Control page 95
Trusted Hosts page 120, 134
trusted interface
assigning static IP addresses on 53
changing IP address of 50
configuring 50—53
configuring additional computers on 53
configuring with Quick Setup Wizard 19
default setting for 33
described 6
Trusted Network Configuration page 50, 51, 52

U

UDP (User Datagram Protocol) 2
Uniform Resource Locator (URL) 4

Update page 42
updating software 31
upgrade options
  activating 42
  viewing status of 24
Upgrade page 43
user accounts
  changing name, password 115
  configuring MUVPN settings 112
  configuring MUVPN settings for all 146
  creating new 113
  deleting 109
  editing 109
  enabling MUVPN access for 147
  read-only administrative 114
  setting WebBlocker profile for 114, 119
  viewing 109
  viewing current 26
  viewing statistics on 26
user authentication. See authentication
user licenses 110
users
  creating 113
  viewing settings for 107
users. See Firebox users

V

View Configuration page 44
virtual adapter, settings for 112, 146
VPN Keep Alive page 142
VPN page
  described 29
  subpages of 30
VPN Statistics page 143
VPNs
  and static IP addresses 143
  described 135
  increasing number allowed 144
  Keep Alive feature 142
  managed, described 136
  manual
    creating 138—142
    described 136, 137
    Phase 1 settings 140

Phase 2 141
special considerations for 135
troubleshooting connections 143
viewing statistics on 143
what you need to create 135

W

wall mounting plate 168
WAN Failover
configuring 60
described 43, 60
using broadband connection for 61
WAN Failover page 61
WAN Failover Setup Wizard 61
WAN ports
described 168
WAN1 60
WAN2 60
WatchGuard Firebox System (WFS)
enabling remote management with 40—41
WatchGuard Logging page 104
WatchGuard Security Event Processor 104
WatchGuard System Manager
enabling remote management with 38—??
setting up access to 38—??
Watchguard System Manager Access page 38
web browser
requirements for 10
settings for 13
Web sites
blocking specific 132
blocking using WebBlocker 121—134
bypassing WebBlocker 132
WebBlocker
allowing sites to bypass 132
bypassing 133
categories for 124—131
creating profiles 123—124
database 121
defining profile 114, 119
WebBlocker page
described 29
subpages of 29

WebBlocker Settings page 122, 123
Wide Area Network (WAN), described 1
Windows 2000, preparing for MUVPN clients 151
Windows 98/ME
  preparing for MUVPN clients 150
Windows NT, preparing for MUVPN clients 150
Windows XP
  installing File and Printer Sharing for Microsoft Networks on 153
  installing Internet Protocol (TCP/IP) Network Component on 153
  preparing for MUVPN clients 152
WINS and DNS settings, configuring 150, 152
wireless card, configuring 74
wireless communication
  antenna directional gain 170
  channel bandwidth 170
  described 169
  path-loss 170
  signal attenuation 170
Wireless Configuration page 67
Wireless Encryption Privacy (WEP) 69
wireless guest services, configuring 72
Wireless Network Connection dialog box 74
Wireless Network Wizard 66
wireless setup 65—75
Wizards page 30
wizards, list of 30

Z

ZoneAlarm
  allowing traffic through 159
  described 145, 159
  icon for 157
  shutting down 160
  uninstalling 160